Haaga-Helia
ammattikorkeakoulu Oy

Maksukorttien riskit

Teo Raittila
Tom Terola

Opinnäytetyö
Finanssi- ja talousasiantuntijan
koulutusohjelma
2018

Tiivistelmä

Haaga-Helia ammattikorkeakoulu Oy

Tekijät
Teo Raittila ja Tom Terola

Koulutusohjelma
Finanssi- ja talousasiantuntijan koulutusohjelma

Opinnäytetyön nimi
Maksukorttien riskit

Sivu- ja liitesivumäärä
48+0

Maksutavat ovat muuttuneet aineellisesta rahankäytöstä aineettomaksi. Nykyajan maksutavoista maksukortti on yksi suosituimmista. Maksukortin käyttöön sisältyy kuitenkin erilaisia riskejä. Opinnäytetyön aiheena on maksukorttien riskit. Tarkoituksena on selvittää, mitkä ovat yleisimmät maksukortteihin liittyvät riskit Suomessa. Alatutkimusaiheena on, miten maksukorttien riskeiltä voi suojautua. Opinnäytetyö toteutettiin vuoden 2018 tammikuun ja huhtikuun välisenä aikana käyttäen apuna pääosin internetistä löytyvää aineistoa. Tavoite oli selvittää yleisimmät maksukorttien riskit ja niitä varten olevat suojautumiskeinot. Lisäksi tavoitteena oli antaa kehitysehdotuksia maksukorttien turvallisuuden parantamiseksi.

Teoriaosassa käydään läpi ensin maksutapojen kehittymistä ja korttimaksamista yleisellä tasolla. Maksutapojen muutoksissa käydään läpi esimerkiksi maksuvälineiden evoluutiota. Maksukorteilla tehtäviä väärinkäytöksiä esitellään luvussa 3 muun muassa skimmaukseen perehtymällä. Empiriaosassa esitellään tutkimusaineisto, joka perustuu julkiseen materiaaliin.

Opinnäytetyö osoittaa, että maksukorttien riskejä ei tule aliarvioida. Riskejä on olemassa ja toiset niistä ovat yleisempiä kuin toiset. Kuitenkin huolellisella kortin käytöllä ja erilaisia turvallisuusohjeita noudattamalla riskien toteutumista voi minimoida. Opinnäytetyö käy läpi yleisimmät riskit ja niiltä suojautumiseksi vaadittavat toimet. Lisäksi käydään läpi erilaisia vastuita liittyen riskien realisoitumiseen. Riskien läpikäyminen ja turvallisuusohjeiden koostaminen auttavat ymmärtämään, kuinka tärkeää on käyttää maksukorttia turvallisesti, ja mahdollistaa riskeiltä välttymisen maksukorttia käyttäessä.

Asiasanat
maksukortit, riskit, turvallisuus, suojautuminen, maksaminen

Sisällys

1 Johdanto

Maksutavat ovat kehittyneet ajan myötä huomattavan paljon. Menneisyyden kolikko- ja seteliajoista on pikkuhiljaa siirrytty moderniin aineettomaan rahaan. Raha vaihtaa omistajaansa digitaalisessa muodossa millisekunneissa. Yksi suosituimmista maksuvälineistä nykyään on maksukortti.

Yhä useammat ostokset eri kaupoissa maksetaan erilaisilla maksukorteilla. Korttien käytön lisääntyessä kasvaa myös kortteihin kohdistuva rikollisuus ja riskien realisoituminen. Rikollisilla on monia keinoja, joiden tavoitteena on aina saada haltuun kortilla olevat tiedot. Tietojen avulla päästään käsiksi kortinhaltijan pankkitilillä oleviin rahoihin. (Poliisi 2018.)

”Maksukortit ovat teknisesti ajateltuna datan- eli tiedonsiirtovälineitä. Maksukorteiksi luetaan esimerkiksi luottokortit, maksuaikakortit, pankkikortit, käteisautomaattikortit ja debitkortit. Niiden käyttö maksuvälineenä perustuu siihen, että jokaisessa kortissa on sen yksilölliseksi tekevä numerosarja. Kortilla tehdyt ostokset tai käteisnostot veloittavat korttiin liitettyä pankki- tai luottotiliä. Useimmissa maksukorteissa on ainakin kaksi rinnakkain olevaa teknistä sovellusta, jotka välittävät maksutapahtumaan tarvittavaa kortin yksilöivää datasisältöä: kortin takapuolella oleva magneettijuova, kortin etupuolella oleva mikrosiru tai kortin etupuolelle painettu kortin numero kohokirjoituksella.” (Poliisi 2018.)

”Siru on uudempaa tekniikkaa, magneettijuova taas vanhaa. Magneettijuovan suojaus kopiointia vastaan on olematon, sirua sen sijaan ei ole tiettävästi kukaan onnistunut kopioimaan. Teknologiaa hyväksikäyttävä rikollisuus ja sen torjunta onkin usein kuin kilpajuoksua: rikolliset yrittävät keksiä teknologisia porsaanreikiä ja maksuliikenneturvallisuutta ylläpitävät tahot yrittävät tukkia niitä. Uusien teknisten sovellusten turvallisuus testataan aina tahtomattakin viime kädessä rikollisten toimesta: löytävätkö rikolliset näitä porsaanreikiä tai tietoturva-aukkoja. Sirun osalta tällaisia ei ole vielä löytynyt. Magneettijuova sen sijaan on vanhana teknisenä sovelluksena haavoittuva.” (Poliisi 2018.)

Eroavia turvallisuusominaisuuksia on kehitetty ja toimintatapoja väärinkäytösten estämiseksi. Useille pankkien maksu- ja luottokorteille voi asettaa maarajauksen, jonka avulla voi estää kortin käytön Suomen ulkopuolella. Maarajaus tunnetaan nimellä geo-blocking. Pankkien asiakkaat voivat ilmoittaa kortin katoamisesta pankin sulkunumeroon. (Taloustaito 2017.)

Tässä opinnäytetyössä tutkitaan maksukorttien riskejä ja turvallisuutta. Aihe on ajankohtainen korttimaksujen yleistyessä enemmän ja enemmän. Korttimaksujen lisääntyessä käteisen määrä maksuvälineenä vähenee. On tärkeää tiedostaa korttimaksamiseen liittyviä riskejä, jotta voi myös kartoittaa suojautumismahdollisuuksia ja turvallisuutta. Mitä enemmän maksukortteja käytetään, sitä enemmän niihin liittyviä riskejä ilmenee. Valitsimme aiheen, koska halusimme selvittää nykyajan maksuliikenteen riskejä ja niiden yleisyyttä korttimaksamisessa. Meitä kiinnosti tietää, minkälainen kehitys maksutavoilla on ollut ja niiden vaikutus riskeihin. Päädyimme myös henkilökohtaisen kiinnostuksen pohjalta tekemään opinnäytetyötä aiheesta. Varsinkin nuorina finanssialan opiskelijoina aihe on sopiva. Kasvu pienestä vain käteistä käyttävästä pojasta yhä enemmän maksukorttia ja mobiilisia rahansiirtosovelluksia käyttäväksi mieheksi on ollut suuri ja on tärkeää ymmärtää muutoksen tuomat hyvät ja huonot puolet sekä mahdolliset riskit.

1.1 Opinnäytetyön tavoitteet ja rajaukset

Opinnäytetyön päätutkimuskysymyksenä on, mitkä ovat yleisimmät maksukortteihin liittyvät riskit. Alatutkimuskysymyksenä on, miten maksukorttien riskeiltä voidaan suojautua.

Tavoitteena on avata lukijalle maksukorttien riskejä Suomessa, käydä läpi kortinhaltijan ja kortinmyöntäjän vastuita väärinkäyttötilanteessa, käsitellä suojautumiskeinoja riskien välttämiseksi sekä antaa lopulta kehitysehdotuksia turvallisuuden lisäämiseksi. Teoriaosuus kertoo oleellisia tietoja suomalaisten maksukäyttäytymisestä liittyen korttimaksamiseen, maksutapojen kehittymisestä Suomessa sekä maksukorttien väärinkäyttötavoista ja turvallisuusominaisuuksista. Työssä annetaan kehitysehdotuksia maksukorttien riskien minimoimiseksi ja turvallisuuden kehittämiseksi. Työn luettuaan lukija ymmärtää maksukortteihin liittyvät yleisimmät riskit ja erilaisia toimintatapoja niiltä suojautumiseksi.

Opinnäytetyö on rajattu koskemaan maantieteellisesti ainoastaan Suomea. Tarkoituksena ei ole selvittää globaalisti maksukorttien riskejä vaan ainoastaan Suomessa yleisimpiä riskejä. Työssä käytetyt esimerkkitapaukset liittyvät Suomeen.

1.2 Tutkimusraportin rakenne

Opinnäytetyömme rakenne noudattaa Haaga-Helia ammattikorkeakoulun pitkän raportin rakennetta. Johdannossa on esitelty päätutkimuskysymys ja alatutkimuskysymys sekä niiden taustat ja rajaukset. Johdantoa seuraa teoriaosuus luvuissa 2 ja 3. Teoriaosuuden jälkeen tulee empiirinen osuus luvussa 4, jossa esitellään tarkemmin myös käytetty tutkimusmenetelmä. Opinnäytetyön päättää luku 5, jossa käydään läpi löydettyjä havaintoja ja tehdään omia johtopäätöksiä aiheeseen liittyen.

Tässä opinnäytetyössä käytettiin tutkimusmenetelmänä laadullista tutkimusta hankkimalla tietoa aineistosta ja tekemällä havaintoja sekä omia johtopäätöksiä asioista. Aineistoa kerättiin pääosin verkkosivuilta löytyvästä materiaalista tammi- ja huhtikuun 2018 välisenä aikana.

2 Maksutapojen kehittyminen ja korttimaksaminen

Tässä luvussa käsitellään maksutapojen kehitystä ja samalla sivutaan maksutapojen kehittymisen lähihistoriaa. Ymmärtämällä maksutapojen kehitystä, saadaan kuva maksukorttien käytön laajuudesta ja suhteesta muihin käytössä oleviin maksuvälineisiin. On tärkeää tietää, kuinka suuri osa erilaisista maksuista on korttimaksuja tai kuinka käytetty maksutapa korttimaksaminen on. Maksukorttien suosio on yhteydessä maksukortteihin liittyviin riskeihin ja rikollisuuteen. Mitä suositumpi maksutapa maksukortit ovat, sitä enemmän on myös mahdollisuuksia joutua väärinkäytösten uhriksi. Ymmärtämällä laajempaa kokonaisuutta on helpompi käsitellä pelkästään maksukortteihin liittyviä kysymyksiä.

2.1 Maksutapojen historiaa

Maksutapana raha on käänteentekevä keksintö, sillä sen avulla voidaan mitata hyödykkeiden arvoa. Kulta ja hopea olivat aikanaan rahan yleisimpiä raaka-aineita. Kolmannen vuosituhannen valuuttaa on digitaalinen raha. Kolikot ja setelit tuskin koskaan katoavat, vaikka niiden käyttö on vähenemässä. Ihminen on kuitenkin aina havitellut rikkauksia. Muun muassa karja, riisi, suola, kaakao ja simpukat olivat pitkään kaupankäynnin vaihtovälineenä ja toimivat niin sanottuna luonnonrahana. Historian himotuin luonnonvara on kuitenkin kulta. Kullan takia on sodittu ja lähdetty uhkarohkeille ristiretkille. Kultakuume sai ihmiset ryntäämään kullankaivuuseen henkensä uhalla. (Yle 2014b.)

Kun kultaa alettiin käyttää valuuttana, alettiin tuotteiden arvo ilmoittaa tiettyinä määrinä kultaa. Muitakin metalleja alettiin käyttämään maksuvälineinä. Ensimmäiset kolikot lyötiin 600-luvulla ennen ajanlaskun alkua Lyydian valtakunnassa, nykyisen Turkin alueella. Paperirahaa käytettiin ensimmäisen kerran Kiinassa 800-luvulla. Paperiraha oli metallirahaa kevyempi ja näin ollen hyödyllisempi. Euroopassa paperiraha tuli käyttöön vasta vuosisatojen päästä. Paperiraha oli tietynlaista merkkirahaa, sillä se edusti tiettyä kultamäärää. (Yle 2014b.)

Rahan kehitys kulkee nykyään kohti aineettomuutta. Enää ei ole tarpeen kuljettaa käteistä taskussa, sillä digitaalinen raha on kolmannen vuosituhannen valuuttaa. Tileillä olevista rahoista merkitään digitaalinen koodi mikrosirulle, muovikortille tai tietokoneen muistiin. Tulevaisuuden ennusteen mukaan ostoksia voi tehdä ilman maksukortteja. Maksaja voidaan tunnistaa jopa sormenjäljestä tai silmän värikalvosta. (Yle 2014b.)

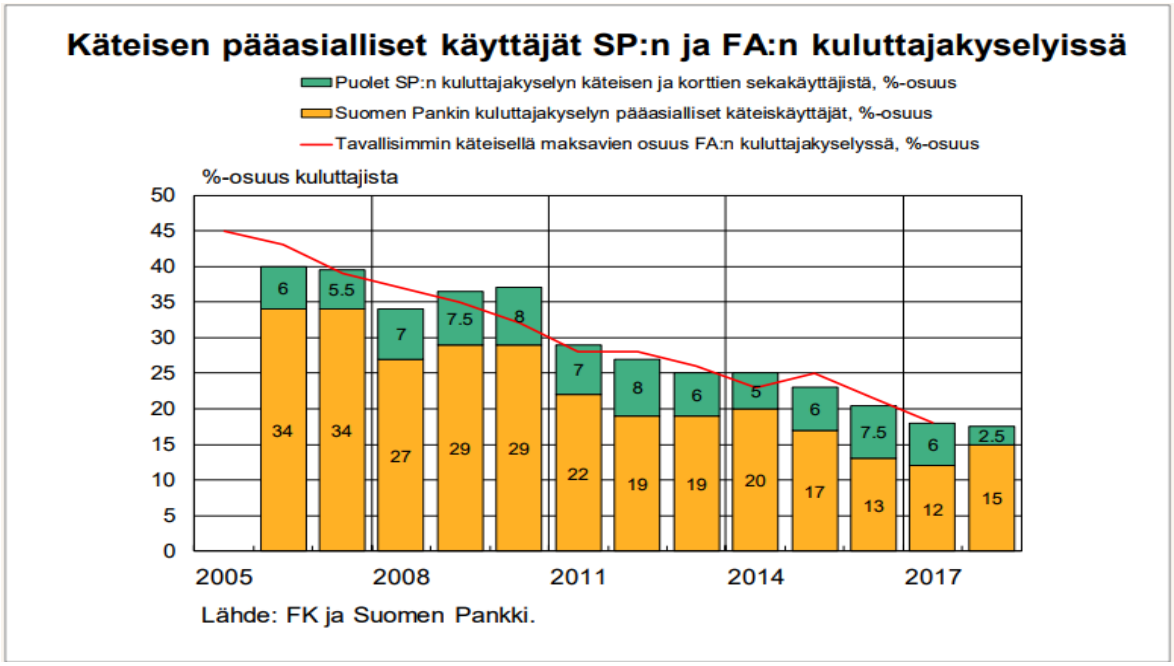
Suomen lainsäädännön mukaan yritys voi itse valita käyttämänsä maksutavat, kunhan niistä ilmoitetaan yrityksen asiakkaille. Käteisestä voi kieltäytyä ja käyttää kaupankäynnissä

maksukorttia, laskua, mobiilimaksua tai vaikka digitaalisia bitcoineja. Suomalaiset ovat alkaneet hyödyntämään elektronista maksamista nopeutuvassa tahdissa. Siihen luetaan pankki- ja luottokortteihin perustuva maksaminen eri muodoissaan sekä mobiilimaksaminen, jossa tavara tai palvelu veloitetaan osana matkapuhelinlaskua. (Profit 2015.)

Yritys säästyy vaihtorahan hankkimiselta sekä käteisen säilyttämiseltä ja sen kuljettamiselta, kun elektroninen maksaminen on käytössä. Käteistä hyödynnetään silloin kun elektronisessa maksamisessa vaadittavat tietoliikenneyhteydet eivät toimi. Pelkästään pankkiautomaattinostoja tehdään vuosittain noin 15 miljardin euron edestä. Yleisesti käteisen käyttö on vähenemässä korttimaksamisen kasvaessa. Vanhemmat ihmiset suosivat yhä käteistä, kun taas elektroninen maksaminen on erityisen suosittu maksutapa 20–34-vuotiaiden keskuudessa. (Profit 2015.)

2.2 Maksutapojen muutos

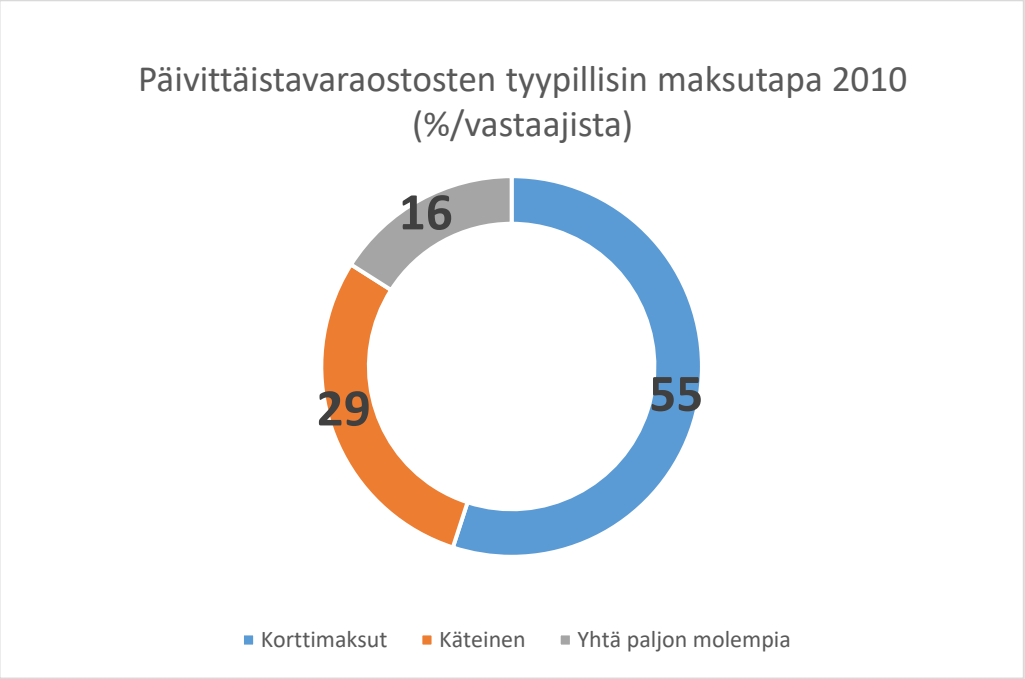
Maksutavat ovat suuressa muutoksessa tänä päivänä ja erityisesti tulevaisuudessa. Suomen Pankin tekemän trendiennusteen mukaan käteisen käyttö vähenee yllättävänkin nopealla tahdilla. Aiemmin on oletettu, että käteinen menettää asemansa 15 vuoden aikana, mutta muutos voi tapahtua paljon nopeammalla aikataululla. Kontaktiton lähimaksaminen on syrjäyttänyt käteismaksujen määrää etenkin pienissä maksuissa. Lähimaksun suurin etu käteiseen verrattuna on nopeus, sillä maksutapahtuma kestää vain muutaman sekunnin, eikä lompakko täyty vaihtorahoista. (Kauppalehti 2016.)



Kaavio 1. Käteisen pääasialliset käyttäjät 2005 – 2017 (SP 2017, 4)

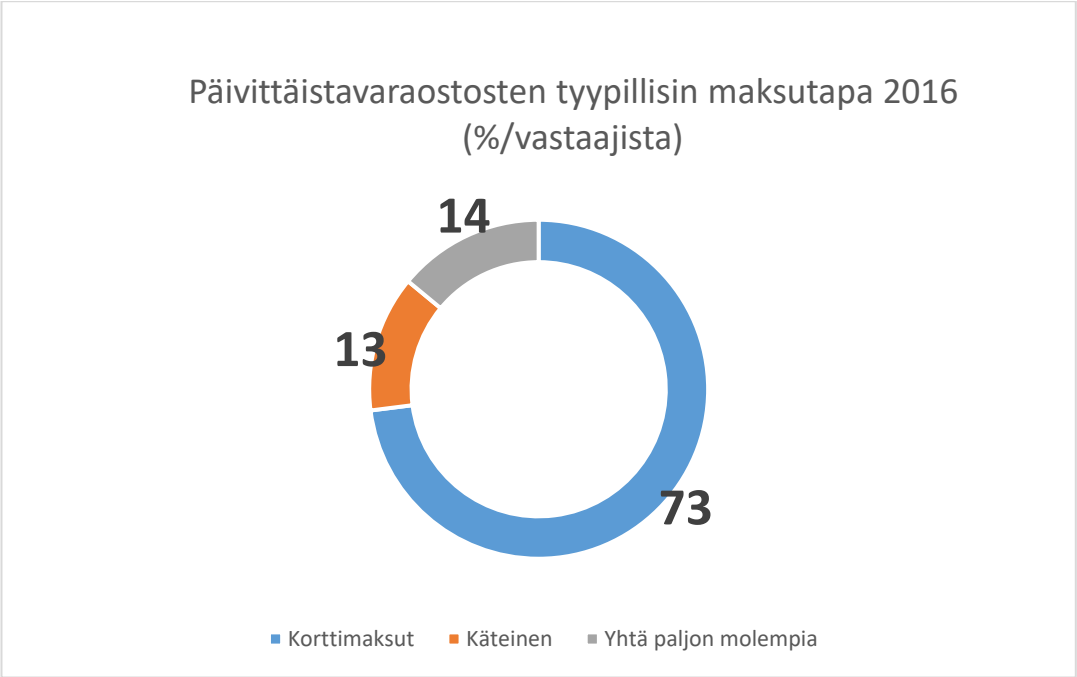
Kaaviosta 1 käy ilmi, että käteisen käyttö on tasaisesti laskenut vuodesta 2005 alkaen. Vuonna 2005 pääasiallisia käteisen käyttäjiä on ollut 34 prosenttia. Vuonna 2017 pääasiallisia käteisen käyttäjiä on ollut vain 12 prosenttia. Kaavio osoittaa sen, että Suomessa ollaan menossa yhä enemmän kohti aineetonta maksamista. (SP 2017, 4.)

Suomen Pankin vuonna 2015 tehdyn kuluttajakyselyn perusteella enää 13 prosenttia kuluttajista pitää käteistä pääasiallisena maksutapana. Kuluttajista 15 prosenttia pitää korttimaksuja ja käteistä yhtä suosiollisina maksutapoina. Käteisen määrän väheneminen näkyy myös rahahuoltoon osallistuvien pankkikorttien määrässä. Vuonna 2005 kyseisiä rahahuoltoon osallistuvia pankkikonttoreita oli lähes 1500, kun vuonna 2016 määrä oli tippunut noin 850 konttoriin. Käteisen määrän väheneminen näkyy lisäksi raha-automaattien määrän vähenemisenä. Vuonna 2015 raha-automaattien määrä väheni 117 kappaleella. Pääosin automaattien sulkemiset johtuivat niiden käytön pienentymisestä. Raha-automaatteja suljettiin vuonna 2015 enemmän kuin muina vuosina yli vuosikymmeneen. (Kauppalehti 2016.)



Kaavio 2. Päivittäistavaraostosten tyypillisin maksutapa 2010 (%/vastaajista) (Kauppalehti 2016)

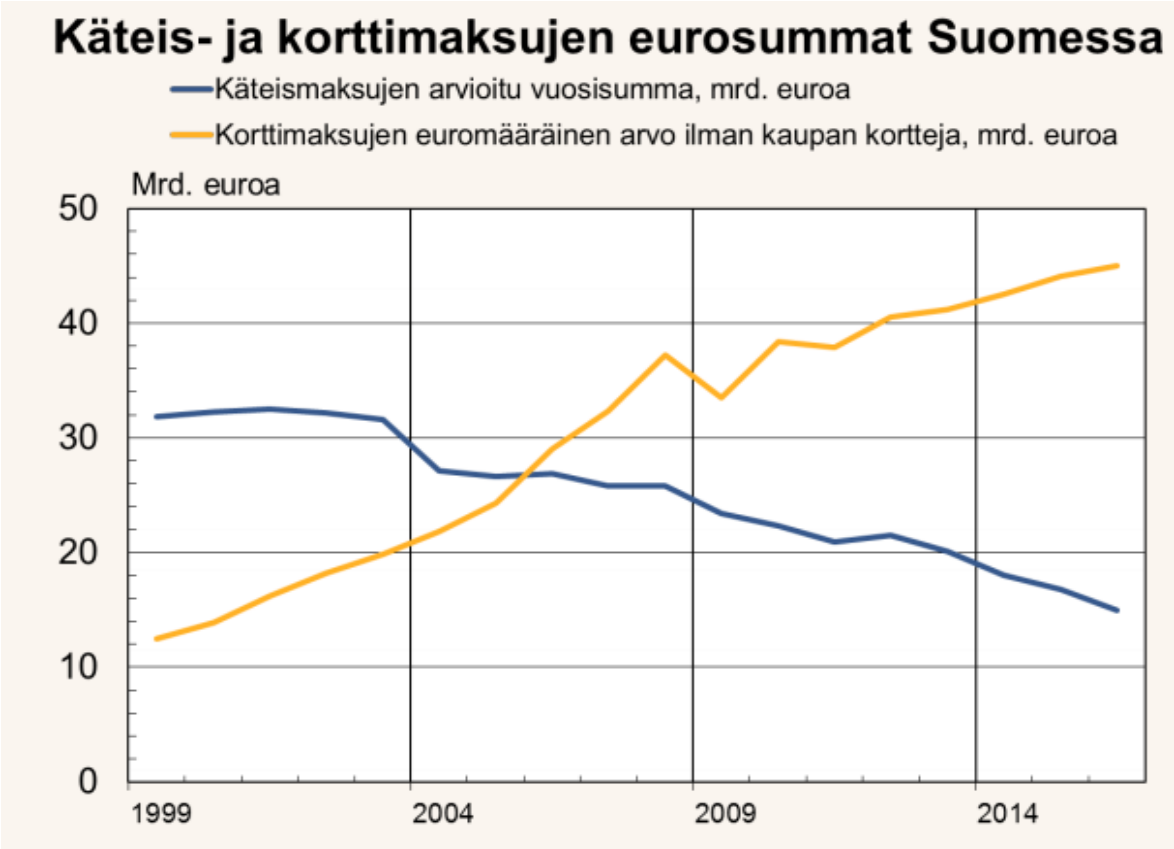
Kaaviosta 2 pystyy havaitsemaan päivittäistavaraostosten tyypillisimmän maksutavan vuonna 2010. Korttimaksu oli ylivoimaisesti suosituin maksutapa, sillä 55 prosenttia vastanneista maksoi päivittäistavaransa maksukortilla. Pelkkä käteinen oli toiseksi suosituin maksutapa 29 prosentin osuudella vastanneista. 16 prosenttia vastanneista käytti yhtä paljon molempia maksutapoja eli käteistä ja korttimaksamista. (Kauppalehti 2016.)



Kaavio 3. Päivittäistavaraostosten tyypillisin maksutapa 2016 (%/vastaajista) (Kauppalehti 2016)

Kaaviosta 3 pystyy havaitsemaan päivittäistavaraostosten tyypillisimmän maksutavan vuonna 2016. Korttimaksaminen oli tuolloinkin ylivoimaisesti suosituin maksuväline 73 prosentin osuudella kaikista vastanneista. Verrattuna vuoteen 2010 korttimaksamisen suosio oli kasvanut 18 prosenttiyksikköä. Toiseksi suosituin maksutapa oli käyttää käteistä ja korttia yhtä paljon, ja niiden osuus oli 14 prosenttia. Käteistä käytti tyypillisimpänä maksutapana enää 13 prosenttia vastanneista. Verrattuna kaavioon 2 eli vuoteen 2010 käteisen suosio oli laskenut 16 prosenttiyksikköä. (Kauppalehti 2016.)

Keväällä 2017 Finanssialan kyselytutkimuksen perusteella 82 prosenttia suomalaisista maksaa ostoksensa tavallisimmin käyttäen jonkunlaista maksukorttia. Verrattuna vuoden 2015 tehtyyn kyselytutkimukseen maksukorteilla maksavien osuus on lisääntynyt selvästi. Vielä vuonna 2015 maksukorteilla maksavia oli 74 prosenttia. Käteisellä maksavien osuus on vähentynyt 7 prosenttiyksiköllä. Käteisellä tavallisimmin ostoksensa maksaa 18 prosenttia vastaajista. (FA 2017, 47.)



Kaavio 4. Käteis- ja korttimaksujen eurosummat Suomessa 1999 – 2016 (SP 2017, 3)

Ihmisten osuus, jotka eivät juurikaan koskaan nosta käteistä on lähes kaksinkertaistunut vuodesta 2015. Yhdeksän prosenttia suomalaisista ilmoittaa, etteivät nosta käteistä juuri koskaan. Keväällä 2015 kyseisten vastaajien osuus oli 5 prosenttia. (FA 2017, 51.) Kaaviosta 4 pystyy havainnoimaan euromääräisen muutoksen korttimaksujen ja käteisen suosiossa. Käteismaksujen määrä on vähentynyt jyrkästi vuoden 1999 noin 32 miljardista eurosta noin 15 miljardiin euroon vuonna 2016. (SP 2017, 3.)

2.3 Korttimaksaminen maksutapana

Maksukortti on nimitys erilaisille maksamiseen ja käteisen rahan nostamiseen tarkoitetuille korteille. Maksukorttien valikoima on laaja ja vaihtelee pankeittain. Erilaisia korttityyppejä ovat credit-, debit-, yhdistelmä- ja prepaidkortit. Tunnuslukuun (PIN) perustuvilla niin sanotuilla sirullisilla maksukorteilla voi tehdä ostoksia ja nostaa rahaa käteisautomaateista koko yhtenäisellä euromaksualueella. Myyjäliikkeet voivat itsenäisesti päättää, mitä kortteja he hyväksyvät maksuvälineenä. Jotkut maksukortit sisältävät myös lähimaksuominaisuuden, jonka avulla voi maksaa pieniä ostoksia viemällä maksukortin lähelle maksupäätettä. Pintunnuslukua ei tarvita. Useimmiten lähimaksuominaisuuden voi kuitenkin poistaa käytöstä niin halutessaan. (Finanssivalvonta 2016.)

Luottokortti eli credit-kortti on maksukortti, jolla kortinhaltija saa luottoyhtiöltä ostoksien tekoa varten luottoa. Luottoyhtiöt saavat tuloja korttien käyttömaksuista, luottojen korosta ja kauppiaan maksamasta provisiosta jokaisesta maksutapahtumasta. Myyjä voi halutessaan lisätä ostoksen loppusummaan luottokortin käytöstä aiheutuvat kulut. Luottokortteja on kahdenlaisia: maksuaikakortteja ja varsinaisia luottokortteja. Maksuaikakortissa koko velkasaldo on maksettava eräpäivänä, kun taas varsinaisessa luottokortissa saldo voidaan maksaa pidemmän ajan kuluessa. Maksuaikakortilla ei peritä erillistä korkoa velasta, kun taas varsinaisella luottokortilla maksettaessa luotosta peritään korkoa. Korteista maksetaan vuosimaksua, tilinhoitomaksuja tai muita kuluja. Luotto-ominaisuuden voi yhdistää toiseen korttiin, jolloin on kyse yhdistelmäkortista. (Kuluttajaliitto 2018.)

Luototon sirullinen pankkikortti eli debit-kortti on kansainvälinen. Debit-kortilla ei voi ostaa luotolla, vaan korttiostot ja automaattinostot veloitetaan suoraan pankkitililtä. Online debit -korteilla (esimerkiksi Visa Electron tai MasterCard Online) tehdyt maksutapahtumat varmennetaan aina. Offline debit -korteilla maksutapahtumat varmennetaan satunnaisesti. Prepaid-korteille raha ladataan etukäteen. (Finanssivalvonta 2016.)

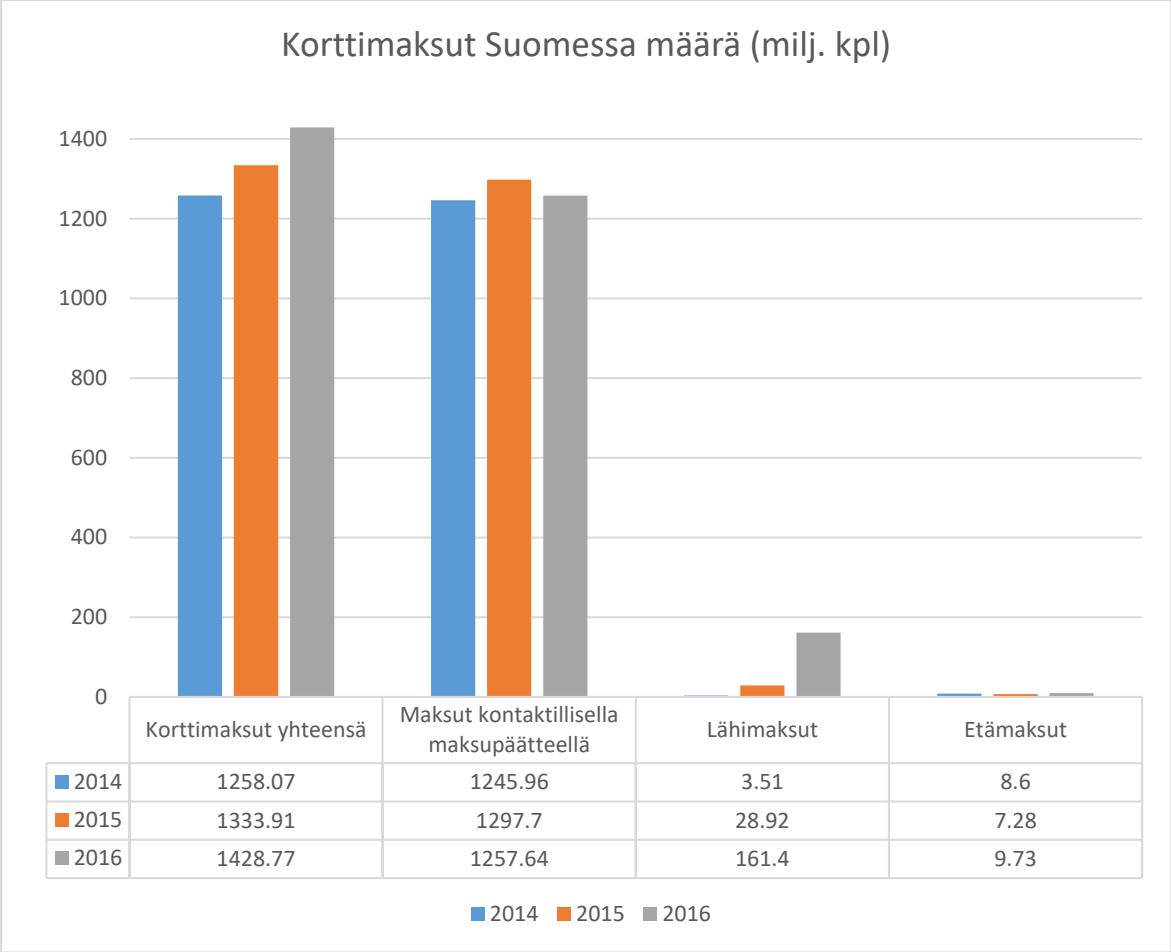
Lähimaksamisessa lähilukuominaisuudella varustetulla kortilla voidaan maksaa pieniä alle 25 euron ostoksia ilman tunnusluvun näppäilyä maksupäätteeseen. Lähimaksaminen tapahtuu käytännössä niin, että maksukortti viedään muutaman senttimetrin päähän maksupäätteestä, jolloin maksu siirtyy kortilta myyjälle. Maksupääte ilmoittaa lähimaksutapahtuman onnistumisesta hyväksyntätekstillä, vihreällä valolla ja sekä tai piippausäänellä. Lähimaksuominaisuudella varustettua maksukorttia voi käyttää myös perinteiseen maksamiseen. Suuremmissa kuin 25 euron ostoksissa maksukortti syötetään perinteiseen tapaan maksupäätteeseen ja pin-koodia käytetään entiseen tapaan. (Korttiturvallisuus 2018c.)

2.4 Korttikäytön tilastoja Suomessa

”Korttimaksaminen on Suomessa ylivoimaisesti mieluisin maksutapa silloin, kun kuluttajalla on mahdollisuus valita. Korttimaksaminen on kuluttajien suosikkimaksutapa myös muualla Pohjolassa. Asiakkaat kokevat korttimaksamisen käteismaksua kätevämpänä ja helpompana maksuvaihtoehtona.” (Nets 2016.)

”Tällä hetkellä 82 prosenttia suomalaisista maksaa ostoksensa tavallisimmin jollakin maksukortilla. Maksukorteilla maksavien osuus on lisääntynyt selvästi keväästä 2015, jolloin maksukorteilla maksavia oli 74 prosenttia. Tavallisimmin debit-ominaisuudella maksavien osuus on kasvanut viidellä prosenttiyksiköllä ja luotto- tai credit-kortilla maksavien kolmella prosenttiyksiköllä. Debit-ominaisuudella maksaminen on nykyisin yleisin maksutapa kaikilla

yli 15-vuotiailla suomalaisilla. Yli 80 prosenttia 18-44-vuotiaista, 75 prosenttia 45–54-vuotiaista, yli 60 prosenttia 55–74-vuotiaista ja alle 18-vuotiaista ja reilut puolet yli 75-vuotiaista maksaa ostoksensa tavallisimmin juuri debit-ominaisuudella.” (FA 2017, 47-51.)



	Korttimaksut yhteensä	Maksut kontaktillisella maksupäätteellä	Lähimaksut	Etämaksut
2014	1258.07	1245.96	3.51	8.6
2015	1333.91	1297.7	28.92	7.28
2016	1428.77	1257.64	161.4	9.73

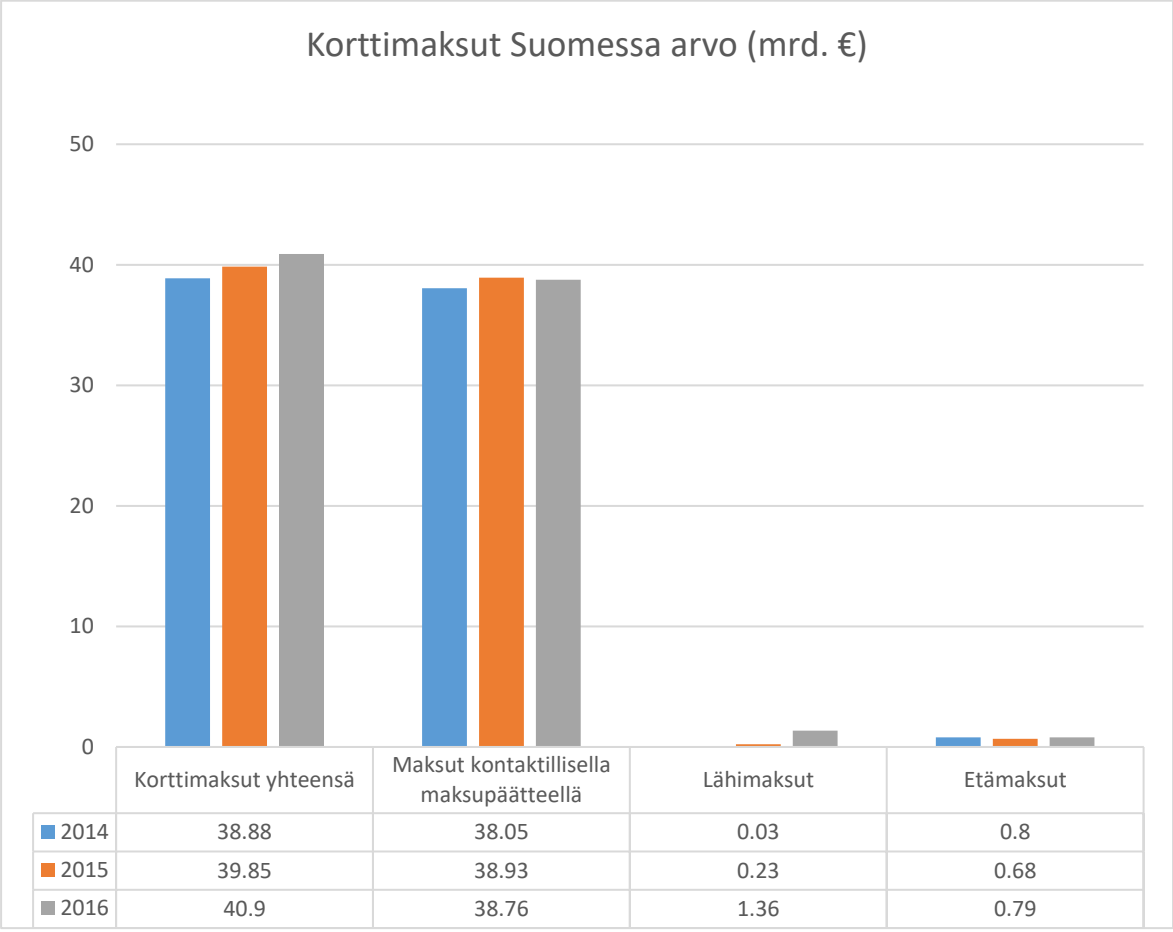
Kaavio 5. Korttimaksut Suomessa määrä (milj. kpl) (SP 2018)

Kaaviosta 5 käy ilmi, että korttimaksujen määrä on kasvanut tasaisesti vuodesta 2014. Vuonna 2014 niitä on ollut 1258,07 miljoonaa kappaletta Suomessa ja vuonna 2016 1528,77 miljoonaa kappaletta. Huomioitavaa on myös lähimaksamisen suosion kasvu. Vuonna 2014 lähimaksuja on tehty 3,51 miljoonaa kappaletta, mutta vuonna 2016 jopa 161,4 miljoonaa kappaletta. Kasvu on melkoinen. (SP 2018.)

”Lähimaksuominaisuus alkaa olla maksukorteissa jo perusominaisuus, ja sen saa korttiinsa automaattisesti. Tällä hetkellä jo lähes kaikilla yli 18-vuotiailla suomalaisilla on käytössään jokin pankin myöntämä maksukortti. Maksukortin omistajien osuus on kasvanut keväästä 2015 kolmella prosenttiyksiköllä ja on nyt 97 prosenttia. Keskimääräistä vähemmän maksukortin omistavia on alle 18-vuotiaiden joukossa, joista pankin myöntämä maksukortti on 88 prosentilla. Tutkimuksen mukaan 64 prosentilla pankin myöntämän maksukortin omaa-

vista suomalaisista on kortissaan lähimaksuominaisuus. Lähimaksuominaisuuden omaavien osuus on lähes kolminkertaistunut keväästä 2015, jolloin se oli 22 prosenttia. Lähimaksuominaisuuden käyttäminen on myös lisääntynyt erittäin selvästi. Tällä hetkellä 81 prosenttia lähimaksuominaisuuden maksukortissaan omaavista on käyttänyt ominaisuutta. Lähimaksuominaisuuden käyttäjiä sen kortissaan omaavista on keskimääräistä merkitsevästi enemmän 18–34-vuotiaiden keskuudessa, joista yli 90 prosenttia on maksanut lähimaksuominaisuudella.” (FA 2017, 47–51.)

”Reilu viidennes suomalaisten verkkokaupoissa tekemistä ostoksista maksetaan luottokortilla, mutta lisäksi neljännes käyttää sitä toissijaisena maksutapana. Lähes yhdeksän kymmenestä suomalaisesta nostaa käteistä rahaa ainakin joskus pankkiautomaatista. Kaupan kassalta käteisen nostaminen on edelleen harvinaista tavallisimpana käteisen nostotapana. Kaupan kassalta käteisen nostaminen on kuitenkin lisänä muiden käteisennostotapojen joukossa, ja vähintään joskus kaupan kassalta nostavien osuus on kasvanut yhdeksästä prosentista yhteentoista prosenttiin.” (FA 2017, 47–51.)



	Korttimaksut yhteensä	Maksut kontaktillisella maksupäätteellä	Lähimaksut	Etämaksut
2014	38.88	38.05	0.03	0.8
2015	39.85	38.93	0.23	0.68
2016	40.9	38.76	1.36	0.79

Kaavio 6. Korttimaksut Suomessa arvo (mrd. €) (SP 2018)

Kaavio 6 kertoo, että korttimaksujen arvo on myös tasaisessa kasvussa. Vuonna 2014 niiden arvo on ollut 38,88 miljardia euroa ja vuonna 2016 40,9 miljardia euroa. Lähimaksamisen arvo on myös kasavanut melkoisesti, sillä vuonna 2014 niiden arvo on ollut 0,03 miljardia euroa, mutta vuonna 2016 1,36 miljardia euroa. (SP 2018.)

2.5 Korttimaksaminen osana digitaalisia maksutapoja

Maksaminen on tullut lähiaikoina uutena ominaisuutena mobiililaitteisiin. Suomalaisten pankkien Pivolla ja Nordea Payllä voi nyt maksaa kaikissa kaupoissa, joissa fyysisen kortin lähimaksukin on tarjolla. Samoin kansainväliset lompakot, kuten Apple Pay, Samsung Pay, Android Pay, ovat jo arkipäivää tietyillä markkinoilla ja saapuvat tulevaisuudessa myös suomalaisten pankkien asiakkaiden saataville. Verkkokaupassa maksutavat vaihtelevat eri mobiiliapplikaatioiden välillä, mutta parhaimmillaan verkko-ostosten kokemus parantuu huomattavasti. (Korttiturvallisuus 2018f.)

Esimerkkinä Danske Bankin MobilePay on helppo ja nopea tapa lähettää ja pyytää rahaa. MobilePayllä voi jakaa esimerkiksi ravintola- tai kahvilalaskun. Rahan lähettäminen ja pyytäminen onnistuu helposti pelkän matkapuhelinnumeron avulla. MobilePay on Suomen käytetyin mobiilimaksusovellus, jonka avulla ostokset verkossa, sovelluksissa ja kaupoissa maksetaan vain yhdellä pyyhkäisyllä. MobilePay on maksuton kaikkien pankkien asiakkaille. (MobilePay 2018.)

KUVA 1. Mobiilimaksamisen suosio kasvaa Suomessa (MyNewsDesk 2017)

Rekisteröintiä varten tarvitaan pankkitunnukset, tilinumero IBAN-muodossa ja Debit- tai Credit-kortin numero. Asiakas voi käyttää minkä tahansa suomalaisen pankin maksukorttia ja tiliä. Kortin tietoja ei ole välttämätöntä antaa vielä rekisteröinnin yhteydessä, vaan ne voi tallentaa koska tahansa myöhemmin. Kun kortin tiedot on tallennettu, voi lähettää rahaa MobilePayllä. (MobilePay 2018.)

Maksaminen mobiilisovelluksilla on tehty turvalliseksi useilla tekniikoilla, jotka tekevät maksutietojen varastamisen kännykästä periaatteessa mahdottomaksi. Kortinhaltijan tunnistaminen on tärkein väärinkäytösten estäjä. Se estää muun kuin oman kännykän käyttämisen maksamiseen. Kun fyysinen kortti käyttää lähinnä vain pin-koodia oikean käyttäjän varmistamiseen, käytetään mobiilimaksuissa useita varmennetapoja, esimerkiksi sormenjälki, ruudunlukituksen avauskoodi, mobiilin pin-koodi ja näiden tapojen kombinaatiot. Mobiilimaksamisen takia on erityisen tärkeää, että käyttäjä pitää hyvää huolta puhelimestaan ja maksamiseen liittyvistä tunnuksista. (Korttiturvallisuus 2018f.)

3 Maksukorteilla tehtävät väärinkäytökset

Tässä luvussa käsitellään maksukorteilla tapahtuvia väärinkäytöksiä. Maksukorteilla tapahtuvat väärinkäytökset liittyvät erittäin läheisesti riskeihin. Väärinkäytökset ovat tapoja hyödyntää maksukorttien riskejä. Ilman riskejä ei olisi väärinkäytöksiä ja toistenpäin. Onkin erittäin tärkeää, että väärinkäytöksiä esitetään tässä kappaleessa. Väärinkäytösten lisäksi kappaleessa tutkitaan tilastoja maksupetoksista, jotka ovat suoraan seurauksia tapahtuneista väärinkäytöksistä. Riskeiltä on mahdollista suojautua ja sitä käsitellään luvussa 3.3.

3.1 Maksukorttien väärinkäyttökeinot

Termi skimmaus tulee englanninkielisestä sanasta skimming. Skimming viittaa luottokortin magneettinauhan kopioimiseen ja myös siihen, että korttilukijan lukupää liukuu pitkin magneettinauhaa lukiessaan nauhalla olevaa korttidataa. Hankkiakseen korttidataa rikolliset asentavat maksukorttiautomaatteihin skimmauslaitteita. Skimmauslaitteita asennetaan etenkin vilkkailla paikoilla oleviin käteisautomaatteihin tai miehittämättömien polttoainejakelupisteiden maksukorttiautomaatteihin. Pyrkimyksenä on saada haltuun ihmisten luottokorttien magneettijuovatieto ja tunnusluku. Skimmauksen tekijöillä on etukäteen suunniteltu ja valmistettu sähkötekninen laite tai laitekokonaisuus, joka asennetaan pankkiautomaattiin alkuperäisten komponenttien päälle manipuloimatta alkuperäistä laitteistoa. Skimmauslaitteeseen tallentuneilla tiedoilla on mahdollista valmistaa väärennettyjä korttikopioita, joilla on mahdollista suorittaa käteisnostoja varsinkin EU-alueen ulkopuolella. (Poliisi 2018.)

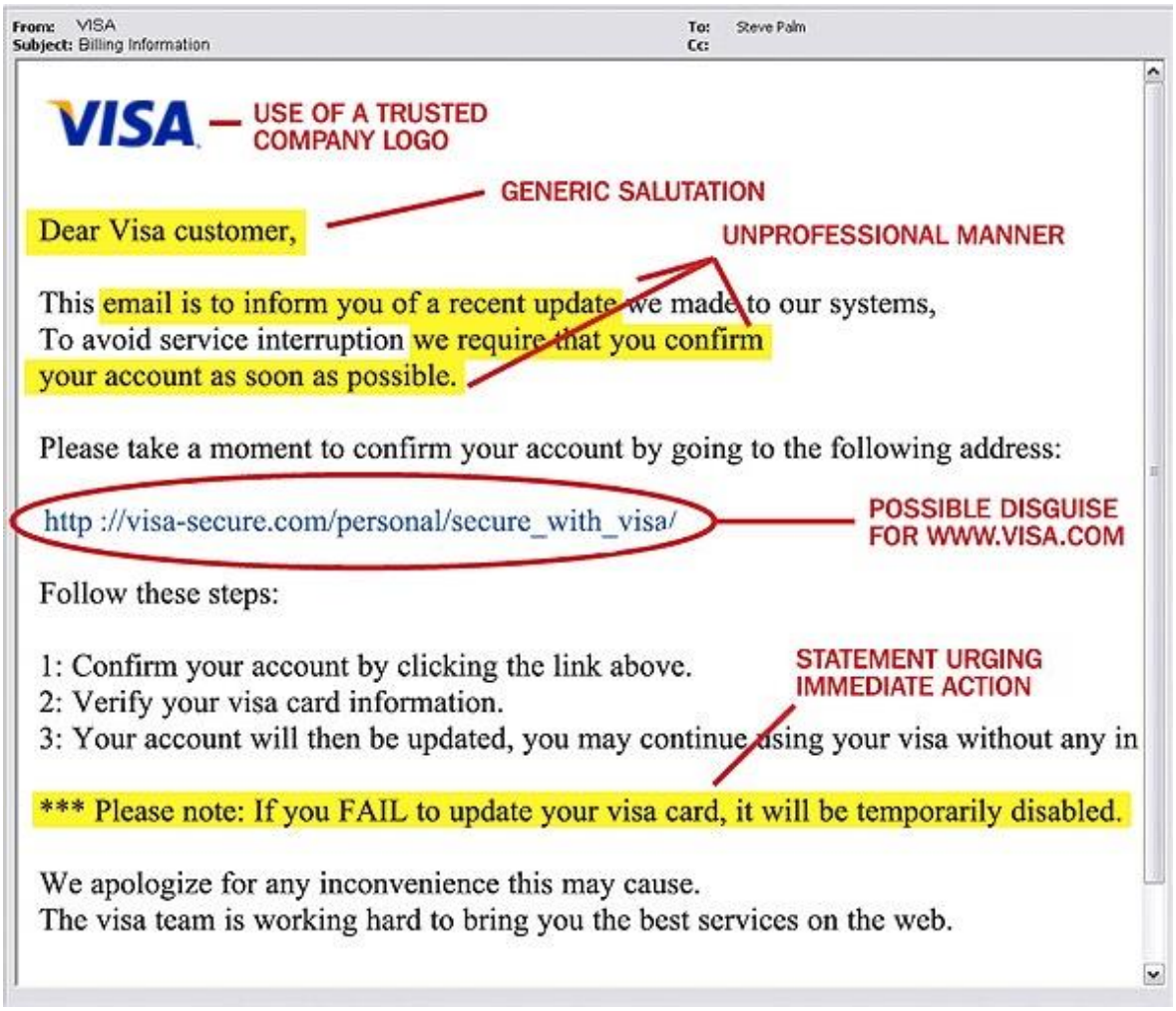
Kuva 2. Esimerkki skimmauslaitteesta (MTV 2013)

”Skimmauslaitteiden suunnittelu ja valmistus tapahtuvat ammattimaisesti Itä- ja Kaakkois-Euroopassa. Useimmiten korttitietojen kopioinnin kaava on seuraava: korttitiedot skimmataan jossakin Euroopan maassa, esimerkiksi Suomessa. Sen jälkeen tiedot lähetetään eteenpäin. Käteisnostojen tapahtumien ulkomailla etenkin EU-alueen ulkopuolella johtuu erityisesti kahdesta syystä.” Ensimmäiseksi kopiointia on vaikeampi jäljittää, kun itse rahan nosto tapahtuu muualla. Toisena syynä on EU:ssa käytössä oleva turvallinen sirutekniikka ja sirukorttiyhteensopivat kortinlukijat. ”Suurin osa rikollisista käteisnostoista tehdäänkin Yhdysvalloissa, jossa magneettijuovan käyttö ilman pin-koodia on edelleen arkipäivää. Vaikka Suomessa on havaittu skimmauslaitteita useita kertoja, on hyvä muistaa, että ilmiö on silti vähentynyt koko EU:n alueella.” (IS 2017.)

Kalasteluviesteissä eli englanninkielisellä termillä phishing tarkoitetaan, että henkilöltä udellaan maksukorttitietoja sähköpostilla ja väärennetyillä verkkosivuilla. Tyypillisiä tunnusmerkkejä ovat (Korttiturvallisuus 2018b.):

- Odottamattoman sähköpostiviestin saaminen.
- Viestin lähettäjä tai sähköpostiosoite on tunnistamaton.
- Lähettäjä saattaa vaikuttaa luotettavalta taholta kuten pankilta.
- Viestiä ei ole osoitettu vastaanottajalle henkilökohtaisesti.
- Viesti on kirjoitettu huonolla suomen tai englannin kielellä.
- Viestissä esimerkiksi varoitetaan turvallisuusuhasta tai teknisestä viasta, joka edellyttää kiireellistä toimintaa
- Viestissä oleva linkki tai verkko-osoite ohjaa sivulle, jossa kysytään luottamuksellisia tietoja.
  (Korttiturvallisuus 2018b.)

Onnistuessaan huijarit yrittävät tyhjentää pankkitilin tai tehdä ostoksia verkossa uhrin rahoilla. (Korttiturvallisuus 2018b.)



Kuva 3. Esimerkki kalasteluviestistä (Oxen Technology 2016)

Maksukortin tietoja voidaan kalastella puhelimella tai tekstiviestillä. Tuntematon henkilö saattaa soittaa puhelimitse ja esittäytyä esimerkiksi pankkivirkailijana tai poliisina. Tuntematon henkilö pyytää antamaan maksukortin numeron ja maksukortin tunnusluvun. Rikolliset käyttävät tekstiviestejä kalasteluvälineenä valikoivammin. Yleisiä kohteita ovat henkilöt, jotka ovat aiemmin luovuttaneet matkapuhelinnumeronsa kalastelusivustolle. Mahdollisesti kohteet valikoituvat satunnaisemmin. Tyypillisesti huijarit lähettävät tekstiviestin, jossa asiakkaalta pyydetään maksukortin tietoja. Eräissä tapatuksissa soittaja pyytää lähettämään määrätyn sisältöisen tekstiviestin. (Nordea 2017.)

Haittaohjelmat ovat ohjelmia, jotka on tarkoituksella tehty vahingoittamaan tietokonetta tai verkkoa. Haittaohjelma on yleiskäsite tietokoneohjelmille, joiden tavoitteena on aiheuttaa epätoivottuja tapahtumia tietokoneessa tai tietojärjestelmissä. Tunnetuimpia haittaohjelmia ovat erilaiset virukset, madot ja vakoiluohjelmat. Tyypillisimmät tavat saada viruksia tieto-

koneelle ovat sähköpostin kautta, ladattaessa tiedostoja verkosta tai pikaviestiohjelman välityksellä. Virukset leviävät myös levykkeiden, kuten cd- ja dvd-levyjen, ja muistitikkujen välityksellä. Haittaohjelmia levitetään lisäksi valheellisten linkkien ja latausten kautta. Yleensä valheelliset linkit ja lataukset esittävät kiinnostavia mainoksia ja lupauksia rajavoitoista. Haittaohjelmat voivat aiheuttaa monia harmeja tietokoneelle. Koneen käyttö voi hidastua sekä internetin selailu ja sähköpostin käyttö voivat hankaloitua. Ohjelmien toiminnassa on mahdollista esiintyä häiriöitä ja tietokone saattaa käynnistyä itsestään uudestaan. Tietokoneen tiedot saattavat hävitä tai muuttua. (Korttiturvallisuus 2018a.) Toisena motiivina haittaohjelmien levittämiselle tietokoneen saastuttamisen lisäksi on saastuneen koneen haltijan maksukorttitietojen saaminen. Haittaohjelmalla on mahdollista urkkia uhrin tietokoneen käyttöä, ja sen kautta saada selville maksukortin tiedot. Lisäksi on mahdollista, että haittaohjelma kysyy korttitietoja. (Nordea 2017.)

Urkinnassa uhrin pin-koodi pyritään saamaan selville, jonka jälkeen maksukortti varastetaan. Vakuutus- ja rahoitusneuvonnan tekemästä Vastuu maksukortin oikeudettomasta käytöstä – Ratkaisukäytäntöä pankin ja asiakkaan välisestä vastuunjaosta -teoksesta löytyy esimerkkejä erilaisista urkintatapauksista. ”Tapauksessa asiakkaan kortin tunnusluku urkittiin asiakkaan oman asioinnin yhteydessä baaritiskillä klo 00:05, asiakkaan lompakko anastettiin ja kortilla tehtiin oikeudettomia nostoja yhteensä 300 euron edestä ennen kuin asiakas teki katoamisilmoituksen kortistaan klo 01:00.” (FINE 2017, 7–8.) Baaritiski ei ole ainoa paikka, jossa voi joutua urkinnan uhriksi: ”Asiakkaan kortin tunnusluku oli urkittu hänen asioidessaan ruokakaupan kassalla. Tämän jälkeen asiakkaan huomio oli parkkipaikalla kiinnitetty toisaalle kysymällä ohjeita kartan kanssa samaan aikaan, kun asiakkaan kortti anastettiin hänen autossaan olleesta ostoskassista.” (FINE 2017, 8.) Urkinnan uhriksi voi joutua myös vilkkaalla paikalla, kuten juna-asemalla: ”Asiakkaan kortin tunnusluku oli urkittu asiakkaan ostaessa juna-aseman lippuautomaatilta matkalippua, minkä jälkeen hänen lompakkonsa anastettiin hänen noustessa junaan. Kortilla tehtiin oikeudettomia automaattinostoja ennen kuin asiakas oli junassa tarkastanut lompakkonsa, havainnut korttinsa puuttuvan ja tehnyt sulkuilmoituksen kortistaan.” (FINE 2017, 9.)

NFC on lyhenne englanninkielisestä lyhenteestä near-field communication. NFC on pankki- ja luottokorttiin lisätty langaton lähimaksuominaisuus. (TM 2017.) NFC mahdollistaa myös väärinkäytökset, sillä lähimaksuominaisuudella varustettu kortti on mahdollista lukea etänä (IL 2017). Kortin tiedot on mahdollista lukea kännykän tai NFC-lähilukulaitteen hipaistessa tarpeeksi läheltä uhrin lompakkoa. Pelkkä pankkikortin vilauttaminen mahdollistaa tietojen kaappauksen kännykkään tai maksupäätteeseen. Tekniikan Maailman testissä tehokkaalla radiolaitteella varustettu rikollinen pystyy lukemaan pankkikortin tiedot suoraan taskussa tai käsilaukussa olevasta lompakosta. (TM 2017.) Kaapatuilla tiedoilla, nimellä, pankkikortin numerolla ja kortin voimassaoloajalla voidaan tehdä ostoksia verkkokaupoissa. Vaikka verkkokauppa vaatisi kolminumeroisen turvaluvun eli niin sanotun CVV-luvun, on sekin mahdollista selvittää. CVV koostuu kolmesta numerosta, joten eri vaihtoehtojen määrä on tuhat. Yksikin ihminen pystyy käymään eri vaihtoehdot läpi alle tunnissa ja tietokoneelta aikaa kuluu vähemmän. (IL 2017.) Kortin tiedot eivät ole ainoa vaarassa oleva asia. Rikollinen voi näppäillä laitteelle halutun summan, lähimaksuissa enintään 25 euroa, ja tilaisuuden tullessa ujuttaa sen edessä olevan henkilön läheisyyteen. Muutamassa sekunnissa rahat vaihtavat omistajaa. Väärinkäytös voi tapahtua baaritiskillä, hississä, ruuhkabussissa, junassa tai liukuportaissa eli yleensä paikoissa, missä liikkuu runsaasti ihmisiä. (TM 2017.)

Kuva 4. Lähimaksullinen maksupääte (American Express 2018)

Digitaalisten tuotteiden lisääntymisestä johtuva tietojen lisääntyvä saatavuus on tuottanut valtavan määrän tietoa yritysten käsiin. Vaikka jotkin tiedot eivät ole vahingoittavia, monet niistä ovat yksityisiä ja arkaluonteisia tietoja yksilöistä ja yrityksistä. Keskittyminen teknologiaan perustuviin työkaluihin, kuten esimerkiksi pilvipalveluihin, on myös helpottanut tietojen saatavuutta, helppokäyttöisyyttä ja vaivattomasti jakamista vähäisillä kustannuksilla. Jotkut väärinkäyttäjät pyrkivät kuitenkin saamaan nämä tiedot käyttöönsä laittomaan toimintaan. Datakaappaus voi tapahtua tahattomasti tai tarkoituksellisesti. Tahaton datakaappaus tapahtuu, kun laillinen tietojenhallitsija, kuten työntekijä, menettää tai käyttää huolimattomasti yrityksen ohjelmia. Työntekijä, joka käyttää suojaamattomia verkkosivustoja, la-

taa pakatun ohjelman työpöydälle, yhdistää salaamattomaan WiFi-verkkoon, menettää kannettavan tietokoneen tai älypuhelimen julkisessa paikassa vaarantaa yrityksen tiedot. (Investopedia 2018.)

Aineellinen datakaappaus tapahtuu, kun hakkeri hyökkää yksilön tai yrityksen järjestelmään, jotta hän pääsee käsiksi yksilön tai yrityksen tietoihin. Hakkerit käyttävät erilaisia tapoja päästäkseen sisälle järjestelmään. Jotkut upottavat haittaohjelmia verkkosivustoihin tai sähköpostin liitetiedostoihin, joita klikkaamalla tai avaamalla tietokonejärjestelmä altistuu hakkereiden yrityksille päästä sisään järjestelmään. Jotkut hakkerit käyttävät botnet-verkkoja, jotka ovat tartunnan saaneita tietokoneita, päästäkseen muiden tietokoneiden tiedostoihin. Botnet-verkkojen avulla tekijät pääsevät useisiin tietokoneisiin samaan aikaan käyttämällä samaa haittaohjelmatyökalua. Hakkerit voivat myös käyttää toimitusketjun hyökkäystä tiedonsaantiin. Kun yrityksellä on vankka ja läpäisemätön suojaustoimenpide, hakkeri voi käydä läpi yhtiön toimitusketjun ja löytää jäsenen, jolla on haavoittuva turvajärjestelmä. Kun hakkeri pääsee haavoittuneen jäsenen tietokonejärjestelmään, hän voi päästä myös kohdeyrityksen verkkoon. (Investopedia 2018.)

Vaikka jotkut tietoverkkorikolliset käyttävät varastettuja tietoa ahdistelemiseen tai rahan kiristämiseen yrityksiltä ja yksityishenkilöiltä, jotkut myyvät rikkoutuneita tietoja maanalaisissa verkkokaupoissa, joissa myydään ja vaihdetaan laitonta omaisuutta. Esimerkkejä myydyistä tuotteista ovat varastetut luottokorttitiedot, liiketoiminnan immateriaalioikeudet, sosiaaliturvatunnukset ja yritysten liikesalaisuudet. (Investopedia 2018.)

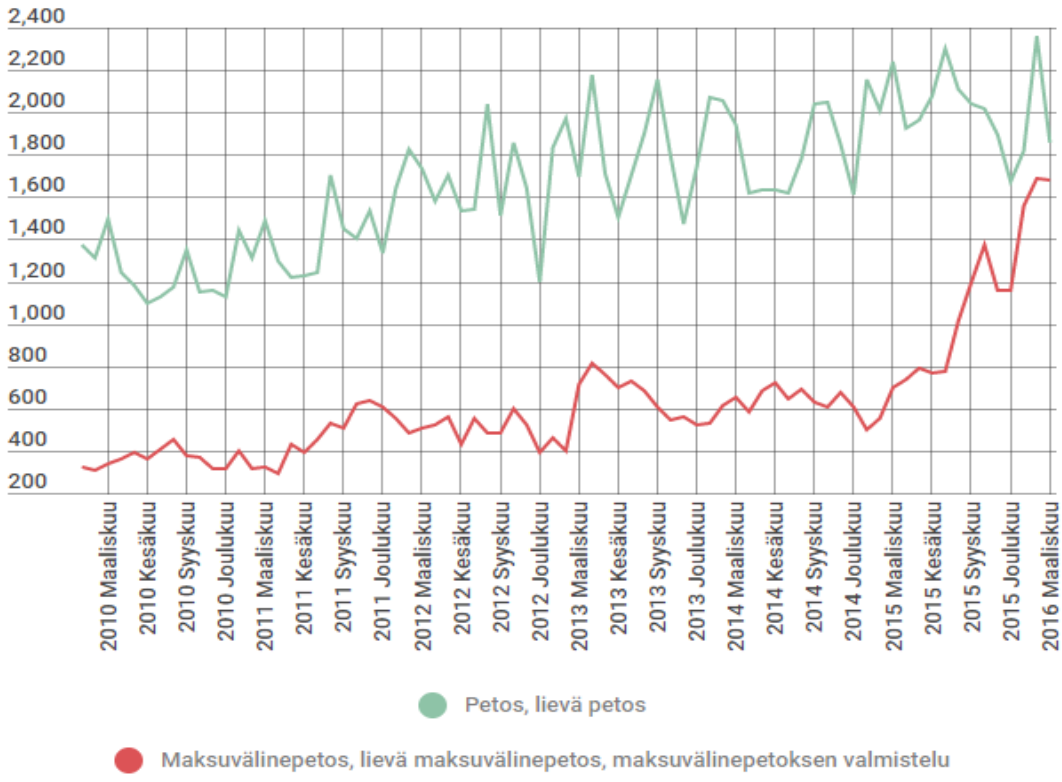
3.2 Tilastoja väärinkäytöksistä

Maksuvälinepetoksen määritelmä on seuraava: ”Mikäli henkilö, hankkiakseen itselleen tai toiselle oikeudetonta taloudellista hyötyä, käyttää maksuvälinettä ilman sen laillisen haltijan lupaa, lupaan perustuvan oikeutensa ylittäen tai muuten ilman laillista oikeutta tai luovuttaa maksuvälineen tai maksuvälinelomakkeen toiselle saattaakseen sen ilman laillista oikeutta käytettäväksi, katsotaan hänen syyllistyvän maksuvälinepetokseen. Maksuvälinepetoksesta tuomitaan myös se, joka tilin katteen tai sovitun enimmäisluottorajan ylittäen väärinkäyttää edellä tarkoitettua maksuvälinettä ja siten aiheuttaa toiselle taloudellista vahinkoa, ellei hänellä maksuvälinettä käyttäessään ollut aikomus viipymättä korvata vahinko. Maksuvälinepetoksesta tuomitaan sakkoa tai vankeutta enintään kaksi vuotta.” (Laki24.fi 2018b.)

Maksuvälinepetos voi olla lisäksi lievä tai törkeä. Lievän maksuvälinepetoksen määritelmä on: ”Mikäli maksuvälinepetos, ottaen huomioon tavoitellun hyödyn tai aiheutetun vahingon

määrä taikka muut rikokseen liittyvät seikat, on kokonaisuutena arvostellen vähäinen, katsotaan teko lieväksi maksuvälinepetokseksi. Lievästä maksuvälinepetoksesta tuomitaan sakkoa.” (Laki24.fi 2018a.) Törkeän maksuvälinepetoksen määritelmä taasen on: ”Mikäli maksuvälinepetoksessa aiheutetaan huomattavaa tai erityisen tuntuvaa vahinkoa tai mikäli rikoksentekijä on rikoksen tekemistä varten tehnyt tai teettänyt maksuvälinelomakkeita, joista rikoksessa käytetty maksuväline on valmistettu, taikka rikos muuten tehdään erityisen suunnitelmallisesti, ja maksuvälinepetos on myös kokonaisuutena arvostellen törkeä, katsotaan teko törkeäksi maksuvälinepetokseksi. Törkeästä maksuvälinepetoksesta tuomitaan vankeutta vähintään neljä kuukautta ja enintään neljä vuotta.” (Laki24.fi 2018c.)

Vuoden 2017 tammi-joulukuussa maksuvälinepetoksia tuli ilmi 6700, mikä on 8 500 tapausta eli 55,9 prosenttia vähemmän kuin vuonna 2016 vastaavana ajankohtana. Törkeitä maksuvälinepetoksia oli 244. Kaikista maksuvälinepetoksista 1800 eli 26,3 prosenttia tehtiin ulkomailla. Edeltävänä vuonna ulkomailla tehtyjen maksuvälinepetosten osuus oli huomattavasti suurempi eli 43,7 prosenttia. Erityisen paljon maksuvälinepetoksia tuli ilmi elokuun 2015 ja elokuun 2016 välisenä ajankohtana. (Tilastokeskus 2017a.) Vuonna 2016 maksuvälinepetoksia tuli ilmi 15 100. Törkeitä maksuvälinepetoksia oli 162. (Tilastokeskus 2017b.)



Kaavio 7. Maksuvälinepetosten, lievien maksuvälinepetosten ja maksuvälinepetosten valmistelun kehittyminen maaliskuusta 2010 maaliskuulle 2016 (MTV 2016)

Kaaviossa 7 havainnollistetaan maksuvälinepetosten, lievien maksuvälinepetosten ja maksuvälinepetosten valmistelun kehittyminen vuoden 2010 maaliskuusta vuoden 2016 maaliskuuhun asti. Maksuvälinepetosten määrä eri muodoissaan on ollut suhteellisen tasaisessa nousussa vertailuajankohdan aikana. Suurempia nousuja on tapahtunut vuoden 2011 aikana, alkuvuodesta 2013, vuoden 2015 aikana ja alkuvuotena 2016. Suurempien nousujen jälkeen on ollut huomattavissa myös selviä laskuja yleensä kohdistuen loppuvuoteen. Maaliskuussa 2010 maksuvälinepetosten, lievien maksuvälinepetosten ja maksuvälinepetosten valmistelujen määrä oli noin 300 kappaletta yhteensä. Maaliskuussa 2016 määrä oli noin 1500 kappaletta. (MTV 2016.)

3.3 Maksukorttien turvallisuus

Kadonneen tai varastetun kortin voi sulkea soittamalla kortinmyöntäjän ilmoittamaan sulkunumeroon, tällöin vastuu kortin sulun jälkeen tapahtuvasta mahdollisesta väärinkäytöstä siirtyy kortinmyöntäjälle. Kortinhaltijan vastuu päättyy sulkuilmoituksen tekemiseen. Suljettua korttia ei tule ottaa uudelleen käyttöön vaikka se myöhemmin löytyisi. Mikäli kortilla on tapahtumia, joita kortinhaltija ei itse ole tehnyt, hän voi tehdä reklamaatiopyynnön kortinmyöntäjälle. Sulkeminen estää kortilla maksamisen. (Korttiturvallisuus 2018j.)

Verified by Visa ja MasterCard SecureCode ovat vahvan tunnistamisen todentamispalveluja, jotka parantavat verkkomaksujen turvallisuutta. Kansainväliset korttiyhtiöt Visa ja MasterCard ovat kehittäneet nämä palvelut. Palvelussa todennetaan ostohetkellä maksutapahtuman molemmat osapuolet: kauppias ja ostaja. Ostoja kannattaa tehdä Visa-korteilla niiden verkkokauppojen sivuilla, joilla on Verified by Visa-symboli ja MasterCard-korteilla niiden verkkokauppojen sivuilla, joilla on MasterCard SecureCode -symboli. Nämä symbolit varmistavat, että kauppias on liittynyt oman pankkinsa kautta palvelun käyttäjäksi. Maksu-

tilanteessa tunnistaudutaan henkilökohtaisilla pankkitunnuksilla tai erillisellä, pankista saadulla varmenteella. Syötetyt tiedot eivät välity kauppiaalle. Kauppias saa vahvistuksen tunnistuksen onnistumisesta myyntilupana. (Korttiturvallisuus 2018h.)

Kuva 5. Verified by Visa ja MasterCard SecureCode (Canadacasino.net 2014)

Vaikka korttien käyttö on turvallista, voivat korttien tiedot joutua vääriin käsiin esimerkiksi tietomurron seurauksena. Väärinkäyttö tapahtuu tavanomaisesti siellä, missä kortin omistaja ei itse ole läsnä. Väärinkäyttö on lisäksi helpointa maissa, joissa on vielä mahdollista käyttää kortin magneettijuovaa eli usein Euroopan ulkopuolella. Maantieteellinen aluerajaus tunnetaan myös nimellä geo-blocking. Se tarkoittaa kortille asetettavaa maantieteellistä rajausta, jonka avulla kortin käyttö voidaan estää Suomen ulkopuolella. Maarajaus koskee pankkikohtaisesti korttimaksamista kaupan maksupäätteillä, automaateilla tai internetissä. Maarajauksen käyttäminen lisää korttiturvallisuutta, koska korttia voi tällöin käyttää ainoastaan kortinhaltijan itse sallimilla alueilla. Maarajauksen avulla on siten esimerkiksi mahdollista estää korttitietojen käyttö ulkomailla, jos itse oleskelee vain kotimaassa. Lomamatkan ajaksi käyttöalueeksi voi rajata vaikkapa loman kohteen. Kortin rajoitusten hallinta onnistuu yleensä verkkopankissa. (Korttiturvallisuus 2018d.)

Myös kortin fyysinen ulkoasu on tärkeä turvallisuutta suunnitellessa. Esimerkiksi jokaisessa MasterCard-kortissa on oltava yksi tai useampi seuraavista turvallisuusominaisuuksista. MasterCard hologrammi näkyy kortin edessä tai takana. Hologrammi on kolmiulotteinen toistuva kuvio, jossa sana MasterCard on painettu taustalle. Kun korttia kallistaa, toistuva kuvio heijastaa valoa ja näyttää liikkuvan. MasterCard HoloMag on holografista magneettinauhaa, jota voidaan käyttää perinteisen magneettiraidan ja MasterCard-hologrammien sijasta. Kaikissa sirukorteissa on EMV-siru, joka mahdollistaa turvallisen maksamisen. MasterCard-kortteissa on oltava häiriösuojattu allekirjoituspaneeli, jossa on toistokuvio. Allekirjoituskenttään on painettu useita värejä, jotka ovat 45 asteen kulmassa valkoisella taustalla laajennettuna. Korteissa on valkoinen kenttä kortin vahvistuskoodille CVC2, jolla vahvennetaan verkko-ostoksia. (MasterCard Card Security Features 2015.)

Kuva 6. MasterCard kortin Holomag (MasterCard Security Features 2015)

Kuva 7. MasterCard-kortin hologrammeja (MasterCard Security Features 2015)

Payment Card Industry Data Security Standards on tietoturvastandardikokoelma, joka on luotu tuomaan lisää tietoturvaa korttimaksamiseen ja määrittelee korttimaksamisen turvallisuuden teknisten vaatimusten minimitason. Se koskettaa satoja miljoonia ihmisiä ympäri maailmaa. PCI DSS:n neuvosto on globaali organisaatio, joka ylläpitää, kehittää ja edistää maksukorttiteollisuuden standardeja kortinhaltijoiden turvallisuuden varmistamiseksi kaikkialla maailmassa. Standardit koskettavat niitä, jotka työskentelevät ja ovat yhteydessä maksukortteihin. Tähän joukkoon kuuluvat kaikenkokoiset kauppiaat, rahoituslaitokset, myyntipisteiden myyjät ja laitteisto- ja ohjelmistokehittäjät, jotka luovat ja käyttävät maailmanlaajuista infrastruktuuria maksujen käsittelyyn. Neuvosto auttaa kauppiaita ja rahoituslaitoksia ymmärtämään ja toteuttamaan turvallisuuskäytäntöjä, teknologioita ja meneillään olevia prosesseja, jotka suojaavat maksujärjestelmiään kortinhaltijoiden tietojen rikkomuksilta ja varastamiselta. Lisäksi neuvosto auttaa myyjiä ymmärtämään ja toteuttamaan turvallisten

maksuratkaisujen luomista koskevia standardeja. Neuvoston perustivat vuonna 2006 American Expressin, Discoverin, JCB Internationalin, MasterCardin ja Visa Inc:n edustajat. Näiden korttiyhtiöiden edustajia on yhä mukana neuvoston työn hallinnossa ja ratkaisujen toteuttamisessa. (PCI Security 2018.)

3.4 Korttitapahtumien valvonta

Esimerkiksi Nets seuraa korttitapahtumia ympäri vuorokauden vuoden jokaisena päivänä korttiväärinkäytön ehkäisemiseksi. Kortinhaltijaan otetaan tarvittaessa yhteyttä tekstiviestillä, kirjeellä tai soittaen. Kortilla voi olla tapahtuma, joka halutaan tarkistaa. Kortti voidaan myös uusia turvallisuussyistä. Nets lähettää kahdenlaisia tekstiviestejä liittyen korttiturvallisuuteen. Viesteissä ei koskaan pyydetä korttinumeroa, tunnuslukua tai muita korttiturvallisuutta vaarantavia tietoja. (Nets 2018.)

Jos kortilla on tapahtuma, joka halutaan tarkistaa, ilmoitetaan asiasta kortinhaltijalle. Kortilla on havaittu maksutapahtuma, joka voi olla väärinkäyttöä, tai epäillään, että kortin tiedot ovat joutuneet vääriin käsiin ja joku muu tekee ostoksia kortilla. Kortinhaltija saa tekstiviestin, jossa pyydetään tunnistamaan maksutapahtuma. Vastaamalla viestiin voi ilmoittaa tunnistaako tapahtuman vai ei. Mikäli tunnistaa maksutapahtuman, voi jatkaa kortin käyttöä normaalisti. Mikäli ei tunnista maksutapahtumaa soitetaan kortinhaltijalle ja selvitetään asiaa yhdessä. (Nets 2018.)

Kortti voidaan myös joutua uusimaan turvallisuussyistä. Kortilla ei ole havaittu väärinkäyttöä, vaan kyseessä on ennaltaehkäisevä toimenpide. Nets on saanut kansainvälisiltä korttiyhtiöiltä tiedon, että korttitiedot ovat mahdollisesti vaarantuneet. Kortinhaltija saa tekstiviestin, jossa ilmoitetaan, että hänelle on tilattu uusi kortti uudella korttinumerolla. Vanhan kortin credit-puoli on tilapäisessä käyttöestossa mahdollisten väärinkäyttöveloitusten ehkäisemiseksi. Mikäli käytössä on yhdistelmäkortti, voi käyttää kortin debit-puolta normaalisti. (Nets 2018.)

Riskien vähentämiseksi pankit käyttävät myös kehittyneempiä teknologioita. Esimerkiksi vertaisvertailuverkoston käyttö yhdessä ulkoisen toimijan kanssa on toimiva ratkaisu. Asiakkaiden tietoja kerätään verkkokauppiailta ja pankeilta, esimerkiksi maksukorttien tietoja, IP-osoitteita ja sähköpostiosoitteita. Kauppiaat ja pankit eivät näe toistensa asiakkaiden yksityiskohtia, mutta voivat arvioida niiden liiketapahtumien riskien tason, esimerkiksi jos luottokortin väärinkäyttöyritys käyttää jatkuvasti samaa IP-osoitetta. Pankit voivat automatisoida datan lähettämisen ulkoiselle toimijalle. Lopulta saadaan muodostettua vertaisvertailuverkosto petosten ehkäisemiseksi. (ComputerWeekly.com 2008.)

Petosten vähentämisen lisäksi verkostojen tarkoituksena on vähentää tarpeettomasti hylättyjen liiketoimien määrää epäillyn petoksen vuoksi ja vähentää petosten hallinnan kustannuksia. Petosten hallinta on kuitenkin edelleen sisäinen prosessi. Järjestelmät käyttävät algoritmeja normaalin korttikäytön mallintamiseen asiakkaan kohdalla ja kohdistavat huomion epänormaaliin käyttäytymiseen, mikä auttaa estämään petoksia. (ComputerWeekly.com 2008.)

4 Maksukorttien riskit

Tässä luvussa käsitellään käytettyä tutkimusmenetelmää sekä esitellään yleisimmät väärinkäyttökeinot. Näin tulee ilmi yleisimmät riskit käytetystä aineistosta esimerkkitapausten muodossa. Lisäksi käydään läpi luvussa 4.3 riskien aiheuttamia vahinkoja ja niihin varautumista ja luvussa 4.4 riskeiltä suojautumista.

4.1 Tutkimusmenetelmän kuvaus

Tässä opinnäytetyössä tutkimusmenetelmänä käytetään kvalitatiivista eli laadullista tutkimusta. Lähtökohtana on todellisen elämän kuvaaminen. Tähän sisältyy ajatus, että todellisuus on moninainen. Tutkimuksessa on myös otettava huomioon, että todellisuutta ei voi pirstoa mielivaltaisesti osiin. Tapahtumat muovaavat samanaikaisesti toinen toistaan, ja onkin mahdollista löytää monen suuntaisia suhteita. Laadullisessa tutkimuksessa yritetään tutkia kohdetta mahdollisimman kokonaisvaltaisesti. Tutkija ei voi sanoutua irti arvolähtökohdista, sillä arvot muovaavat sitä, miten tutkittavia ilmiöitä pyritään ymmärtämään. Objektiivisuutta ei voi saavuttaa traditionaalisessa mielessä, sillä tutkija ja se, mitä tiedetään, kietoutuvat saumattomasti toisiinsa. Yleisesti voidaan todeta, että laadullisessa tutkimuksessa pyritään löytämään tai paljastamaan tosiasioita. (Hirsjärvi, Remes & Sajavaara 1997, 161.)

> Tyypillisiä piirteitä laadullisessa tutkimuksessa ovat esimerkiksi (Hirsjärvi ym. 1997, 164.):
>
> - ”Tutkimus on luonteeltaan kokonaisvaltaista tiedonhankintaa, ja aineisto kootaan luonnollisissa, todellisissa tilanteissa.”
> - ”Suositaan ihmisiä tiedonkeruun instrumenttina. Tutkija luottaa enemmän omiin havaintoihinsa ja keskusteluihin tutkittaviensa kanssa kuin mittausvälineillä hankittavaan tietoon.”
> - ”Käytetään induktiivista analyysiä. Tutkijan pyrkimyksenä on paljastaa odottamattomia seikkoja.”
> - ”Tutkimussuunnitelma muotoutuu tutkimuksen edetessä. Tutkimus toteutetaan joustavasti ja suunnitelmia muutetaan olosuhteiden mukaisesti.”
>
> (Hirsjärvi ym. 1997, 164.)

Valitsimme laadullisen tutkimuksen, koska se sopii paremmin opinnäytetyömme päätutkimuskysymyksen selvittämiseen. Tutkimuksemme on ollut kokonaisvaltaista tiedonhankintaa, aineistoa on koottu todellisista asioista.

4.2 Yleisimmät maksukorttien väärinkäyttötavat

Taulukko 1. Yleisimmät maksukorttien väärinkäyttötavat (Poliisi 2018.)

Yleisimmät maksukorttien väärinkäyttötavat
1. ”Maksukorttien numeroiden ja muiden tunnistetietojen kopioiminen haittaohjelmilla internetissä. Korteilla tilataan nettikaupoista helposti rahaksi muutettavaa tavaraa tai lentolippuja.”
2. ”Maksukorttien magneettinauhoja kopioidaan korttiautomaateilla. Toimintaa kutsutaan skimmaukseksi. Skimmatuilla korteilla yritetään nostaa käteistä rahaa.”
3. ”Kopioiduista korttitiedoista tehdään aidon näköisiä luottokorttiväärennöksiä, joilla ostetaan tavaraa kaupan tiskillä.”
4. ”Automaatilla asioivan kansalaisen PIN-koodi kurkitaan olan yli hänen sitä näppäillessään ja tämän jälkeen hänen maksukorttinsa varastetaan hämäystä käyttämällä. Varastetulla kortilla nostetaan käteistä automaatilta.”

Kuten olemme aiemmin teoriaosiossa käyneet läpi erilaisia maksukorttien väärinkäyttökeinoja, osa niistä on yleisimpiä kuin toiset. Oheisessa taulukossa 1 on poliisin tietojen perusteella neljä yleisintä väärinkäyttökeinoa Suomessa. Käymme seuraavaksi läpi jokaista tapaa esimerkkitapauksien avulla.

4.2.1 Korttitietojen kopioiminen internetissä

”Viitasaarelainen perheenäiti Katja Lindlöf sai vuonna 2013 yllättävän puhelun. ”Sain puhelun Netsistä. He kysyivät, olenko pelannut viime yönä nettipokeria”, sanoo Lindlöf. Perheenäiti ei ollut harrastanut ikinä nettipokeria. Selvisi, että luottokortin tiedot olivat päätyneet vääriin käsiin niin, että hakkeri on päässyt niihin käsiksi tietomurrolla. Korttitietojen hakkerointi vaikutti liittyvän ihan tavalliseen hotellivaraukseen, jonka Lindlöf oli tehnyt netissä aikaisemmin. ”Pääosin maksukorttien tiedot lähtevät vääriin käsiin tavalla tai toisella interne-

tin kautta”, sanoo rikosylikonstaapeli Tero Toivonen Keskusrikospoliisista. ”Rikolliset syöttävät haittaohjelmia ihmisten kotikoneille tai he hakkeroivat palvelimen, jossa on korttitietoja.” ” (Yle 2014a.)

”Koko maailmassa saatetaan hakkeroida jopa satoja miljoonia korttitietoja vuosittain. Yksittäinen tietomurto saattaa poikia jopa 40 miljoonan luottokortin tiedot. Rikolliset myyvät korttitietoja eteenpäin netissä, mutta eivät välttämättä pääse hyödyntämään haltuunsa saamaa korttitietoa mitenkään ja jos pääsevät, ei vastuu vahingosta ole yleensä kortin haltijan.” (Yle 2014a.)

”Luottokorttien käyttöä vahditaan ympäri vuorokauden. Katja Lindlöfin tapauksessa rikolliset eivät kuitanneet voittoja sieppaamillaan korttitietiedoilla, kiitos korttimaksuja pyörittävien operaattorien valppauden. Valvonta toimii tietojärjestelmäpohjaisesti ja seuraa maksutapahtumia. Yritys pelata nettipokeria poikkesi niin paljon kortin aikaisemmasta käytöstä, että maksuoperaattorien järjestelmät hälyttivät ja estivät pelin. Suomalaisten luottokorttien maksuliikennettä pyörittävän Netsin mukaan korttien käyttöä todellakin valvotaan ympäri vuorokauden ihmisvoimin. ”Systeemi toimii tietojärjestelmäpohjaisesti ja seuraa maksutapahtumia. Jos siellä havaitaan tavanomaisuudesta poikkeavaa, järjestelmä hälyttää”, sanoo palvelutuotannon johtaja Jukka Ruotsalainen Netsistä. Tämän jälkeen Netsin työntekijä saattaa olla kortinhaltijaan yhteydessä ja ottaa selvää, onko kyseessä asianmukainen ostos. Hälytys voi liittyä esimerkiksi tilanteeseen, jossa korttia yritetään käyttää lyhyen ajan sisällä maantieteellisesti hyvin kaukana toisistaan olevissa paikoissa.” (Yle 2014a.)

Vuonna 2016 Suomessa paljastui ennätyslaaja maksukorttihuijaus: Kymmenhenkinen joukko nettihuijareita osti 170 verkkokaupasta eri puolilta maailmaa yhteensä yli 130 000 euron arvosta kaikenlaisia tuotteita. Kyseessä on todennäköisesti maksuvälinepetos. Ryhmä asui Suomessa ja tunsi toisensa jotenkuten. Osalla oli ollut keskenään tiiviimmätkin yhteydet, mutta poliisin mukaan kyseessä on hyvin löyhä rinki, ei niinkään järjestäytynyt rikollinen organisaatio. Ostoksia saatiin tehtyä yli 130 000 euron edestä, mutta kaikki ostosyritykset eivät olleet onnistuneita. Huijarit olivat yrittäneet kaiken kaikkiaan ostaa tavaraa verkkokaupoista miljoonalla eurolla. Ostoksiin käytettiin varastettuja maksukorttitietoja. (VertaaEnsin 2016.)

Luottokortteja ei varastettu fyysisesti, vaan varkaat olivat hyödyntäneet korttien tietoja. Ostoksia netissä tehtaillut joukko ei kuitenkaan ollut itse varastanut maksukorttien tietoja vaan hankkinut tiedot netistä. Internetissä kaupataan maksukorttien tietoja erilaisilla rikollisten

suosimilla hämärillä foorumeilla ja suljetuissa verkoissa. Maksukorttien tiedot ovat todellisesti rahanarvoisia, joten kortinhaltijan on oltava tarkkana, etteivät oman kortin tiedot joudu ulkopuolisten tietoon. (VertaaEnsin 2016.)

Myös yritykset käyvät kilpailua varkaiden kanssa teknologisista applikaatioista. Esimerkiksi Ranskassa on nyt tarjolla maksukortteja, joiden viimeiset turvanumerot vaihtelevat muutaman tunnin aikana. Näin varkaat eivät periaatteessa pysty hyödyntämään korttien tietoja, sillä ne vanhenevat vauhdilla. Tällaisista petoksista kärsivät niin kuluttajat, verkkokaupat kuin luottokorttiyhtiötkin. Suurimpia häviäjiä ovat yleensä käytännössä luottokorttiyhtiöt, sillä ne joutuvat usein korvaamaan kuluttajille heidän menettämiään rahoja takaisin. (VertaaEnsin 2016.)

4.2.2 Korttitietojen kopioiminen automaatilla (Skimmaus)

”Vaikka skimmaus on Suomessa vähäistä, poikkeuksellista se ei ole. Suomesta löytyneistä skimmauslaitteista on uutisoitu runsaasti. Elokuussa 2017 Helsingin poliisi otti kiinni miehen, jonka epäillään asentaneen skimmauslaitteita Tampereelle, Pirkkalaan ja Vaajakoskelle. Laitteet löytyivät huoltoasemilta. Maaliskuussa 2017 Vantaalla havaittiin skimmauslaite Tammiston Nesteen maksuautomaatissa. Suomessa skimmauslaitteita on löydetty usein kylmäasemilta. Kylmäasemien lisäksi kopiointilaitteita asetetaan vilkkaasti liikennöityihin raha-automaatteihin. Samassa kuussa korttitietoja yritettiin kopioida myös Hyvinkäällä. Laite oli kiinnitetty kaksipuoleisella teipillä huoltoaseman maksuautomaattiin. Korttitiedot eivät päätyneet eteenpäin, sillä poliisi sai tiedon nopeasti. Salossa vastaavaa petosta yritettiin helmikuussa. Kylmäasemaan kiinnitetty skimmauslaite kiinnitti huomion, sillä se roikkui osittain irti.” (IS 2017.)

”Loka-marraskuussa 2016 Helsingin poliisilaitos selvitti maksuvälinepetossarjaa. Usealta pääkaupunkiseudun huoltoasemalta kopioituja korttitietoja oli hyödynnetty Filippiineillä. Kuudella kortilla oli tehty käteisnostoja. Syyskuussa 2016 skimmauslaitteita löytyi Raumalta ja Turusta Teboil-huoltoasemilta. Heinäkuussa 2016 Espoon käräjäoikeus tuomitsi kaksi bulgarialaismiestä 2,5 vuoden vankeustuomioon seitsemästä maksuvälinepetoksen valmistelusta ja yhdeksästä maksuvälinepetoksesta. Tuomiot tulivat pankkiautomaatteihin asennetuista skimmauslaitteista. Miehet tallensivat 765 henkilön korttitiedot. Toukokuussa 2016 Päijät-Hämeen käräjäoikeus vangitsi myös romanialaismiehen epäiltynä todennäköisin syin epäiltynä neljästä törkeästä maksuvälinepetoksesta. Kopioiduilla maksukorteilla oli nostettu rahaa kymmeniä tuhansia euroja.” (IS 2017.)

”Vuonna 2017 Lounais-Suomen poliisi tutki Salon Hämeentiellä sijaitsevalla huoltoasemalla tehtyä maksuvälinepetosta. Kylmäasemalta löytyi maksukorttien kopiointiin tarkoitettu skimmauslaite. Poliisin mukaan laite muistutti oikeaa kortinlukijaa, mutta lukijassa oleva kortin kuva poikkesi alkuperäisestä. Kortinlukija oli myös jonkun verran irti, ja sen alta paljastui oikea kortinlukija.” (Yle 2017b.)

”Vuonna 2018 Sisä-Suomen poliisilaitos tiedotti tutkivansa yli neljänkymmenen maksuvälinepetoksen sarjaa, jossa pankkikorttien tietoja on käytetty luvatta Indonesiassa. Poliisi epäilee pankkikorttien skimmausta, jossa korttien tiedot olisi saatu haltuun korttiautomaattiin kiinnitetyn kopiointilaitteen ja kameran avulla.” (IS 2018.)

”Skimmausten poliisi epäilee tapahtuneen jo kesällä 2017 Keski-Suomen alueella. Iso osa rikoksista tuli poliisin tietoon marraskuussa. Seuraavan kerran epäilyjä ilmeni maaliskuussa. Tämänkaltaiset rikokset tapahtuvat usein pitkällä aikajänteellä. Joskus pankkikortin tiedot on kopioitu kuukausia tai jopa vuosia aiemmin. Tekijät ovat usein ulkomaalaisia ja poistuvat nopeasti maasta tiedot kopioituaan. Mikäli kopiointi on tapahtunut paljon maksuvälinepetosta aikaisemmin, poliisin keinot ovat vähissä.” (IS 2018.)

4.2.3 Aidonnäköiset korttiväärennökset

Rikolliset koittavat saada haltuunsa korttien identiteettiä yksilöivän datan. Erityisesti maksukorttien sisältämät tiedot ovat kiinnostavia rikollisille. Korttidataa hankitaan muun muassa internetissä haittaohjelmilla, kuten luvussa 3.1 on käyty läpi, ja maksukorttiautomaatteja manipuloimalle eli esimerkiksi asentamalla skimmauslaitteen automaattiin. Jos rikolliset onnistuvat hankkimaan maksukorttidataa tai korttinumeroita, he voivat valmistaa väärennettyjä luottokortteja, joilla voidaan tehdä ostoksia tai suorittaa käteisnostoja. Kyseessä on valtioiden rajat ylittävä rikollisuus, jossa on huomattavia hyötymismahdollisuuksia. Lähes poikkeuksetta kyseiset rikolliset kuuluvat organisoituihin rikollisryhmiin. (Poliisi 2018.)

Ensimmäisenä esimerkkinä korttiväärennöksistä on tapaus, jossa bulgarialaismiehet olivat asentaneet skimmauslaitteita useisiin pankkiautomaatteihin eri paikkakunnilla. Kyseessä oli laaja tapaus ulottuen Vaasasta Rovaniemelle. Skimmauslaitteiden avulla saaduilla korttitiedoilla oli valmistettu korttiväärennöksiä. Kyseisiä korttiväärennöksiä oli käytetty käteisvarojen nostoon Yhdysvaltojen Chicagossa. Nostoja oli suoritettu kymmenien tuhansien eurojen edestä. Vaikka itse nostot ovat tapahtuneet Chicagossa, on itse korttidatan hankkiminen tapahtunut Suomessa. (MTV 2012.) Näin ollen on perusteltua käyttää kyseistä esimerkkiä, vaikka opinnäytetyö on rajattu koskemaan maantieteellisesti vain Suomea.

Toisena esimerkkinä Keski-Suomessa tapahtunut maksukorttien kopiointi. Kortteja oli kopioitu ainakin Jyväskylän, Laukaan, Tikkakosken, Suolahden ja Äänekosken alueilla. Kopioinnit oli suoritettu joko skimmauslaietta käyttämällä tai urkkimalla esimerkiksi rahannoston tai kauppamaksun yhteydessä. Kopioiduilla pankkikorteilla oli suoritettu nostoja Aasiassa. Uutisen julkaisun aikaan asianomistajia oli 26. Esimerkiksi jyväskyläläinen opiskelija oli huomannut tilitiedoista 80 euron noston Kiinassa. (Yle 2017a.) Samoin kuin ensimmäisessä esimerkissä korttien kopiointi oli suoritettu Suomessa, joten maantieteellisestä rajauksesta huolimatta on perusteltua käyttää kyseistä esimerkkiä.

4.2.4 Pin-koodin urkinta ja kortin varastaminen

On useita eri tapoja urkkia henkilön pin-koodi ja varastaa maksukortti. Poliisi on listannut yleisimpiä esimerkkejä, joissa urkitaan pin-koodi, varastetaan kortti tai kokonainen lompakko, jossa maksukorttia yleensä säilytetään. Joissakin tapauksissa toteutetaan molemmat toimenpiteet eli urkitaan pin-koodi ja varastetaan maksukortti. (Helsingin Uutiset 2016.)

Yleisin tapa on pin-koodin urkkiminen ja pankissa tai pankkiautomaatilla vierailleen henkilön seuraaminen. Kyseiset tapaukset kohdistuvat useimmiten yöllä tai aamuyöllä ravintolan tikeillä oleviin päihtyneisiin tai päiväsaikaan kaupoissa asioiviin ikäihmisiin. Huijarit urkkivat pin-koodin, jonka jälkeen he harhauttavat uhria ja varastavat uhrin lompakon. (Helsingin Uutiset 2016.)

Yleinen tapa on setelin tai kolikoiden heittäminen maahan pankkiautomaatilla. Uhrin suorittaessa käteisnostoa hänen yleensä jalkojen juureen heitetään seteli tai kolikoita, taputetaan olkapäälle ja sanotaan, että ”tuo taisi pudota sinulta.” Uhrin kumartuessa poimimaan setelin tai kolikot hänen pankkikorttinsa anastetaan. (Helsingin Uutiset 2016.)

Rikollinen voi esiintyä myös valepoliisina. Tämä harhautus kohdistuu erityisesti ulkomaalaisiin turisteihin, joilla ei välttämättä ole tarkkaa hahmotelmaa aidosta suomalaisesta poliisista. Valepoliisit kertovat epäilevänsä turistia rikoksesta ja haluavat tarkistaa lompakon. (Helsingin Uutiset 2016.)

Lompakon tarkastuksen yhteydessä varastetaan rahat. On myös mahdollista varastaa maksukortti. Tahraaminen on yksi keino suorittaa varkaus. Uhrin päälle heitetään likaista mönjää, jota varkaat alkavat puhdistamaan. Samalla lompakko vaihtaa omistajaa taskusta tai käsilaukusta. Rikolliset voivat myös pyytää uhria kuvaamaan heitä esimerkiksi turistinähtävyyden luona. Kun uhri keskittyy kuvaamiseen, lompakko varastetaan. Rikolliset voivat

viedä tuolin selkänojalla olevasta takintaskusta arvotavaroita. Huijarit istahtavat uhrin takana olevaan pöytään ja vievät uhrin selkänojalla roikkuvan takin taskusta esimerkiksi lompakon. (Helsingin Uutiset 2016.)

Lähikontaktia kannattaa välttää ruuhkassa. Rikolliset aiheuttavat ruuhkaa ja varastavat samalla arvo-omaisuutta. Esimerkiksi rullaportaissa uhrin edessä oleva huijari on pudottavinaan jotain ja jää vetolaukkunsa kanssa jumiin rullaportaisiin. Takaa tuleva rikollinen varastaa uhrin omaisuutta. Tapa on yleinen myös junissa ja raitiovaunuissa. Tiedossa on lisäksi tapauksia, jossa tekijät halaavat uhria ja halauksen yhteydessä tyhjentävät uhrin taskut. (Helsingin Uutiset 2016.)

Yksi yleisimmistä tavoista on lapulla hämääminen tai kaulahuivilla tai takilla peittäminen. Rikolliset peittävät toisen kätensä kaulahuivilla tai takilla, liimautuvat uhrin kylkeen kiinni ja varastavat lompakon, jonka he sitten piilottavat kädessään roikkuvan takin alle. Monesti uhri ei huomaa tekoa ollenkaan. (Helsingin Uutiset 2016.)

4.3 Riskeihin varautuminen ja niiden aiheuttamat vahingot

Luottokorttitietojen väärinkäyttö vaikuttaa rahallisesti kortin haltijaan vain hyvin harvoin. Jos kortin tiedot on kaapattu internetissä omistajan tietämättä, omistaja ei ole syyllistynyt huolimattomuuteen eikä ole tappioista vastuussa. Mahdolliset rikolliset veloitukset korvaa kortin myöntäjä. Luottokorttimaksuissa myös kuluttajansuoja on hyvä. Mikäli verkon kautta ostettua tuotetta ei tule tai se ei vastaa kuvausta, voi asiakas reklamoida asiasta kortin myöntäjälle ja saada rahansa takaisin. (Karjalainen 2015.)

Jos kortin käyttäjä on ollut huolellinen, hän ei joudu tappioita maksamaan. Pääsääntöisesti pankit korvaavat tappiot. Finanssialan keskusliiton mukaan puhutaan vuosittain miljoonista euroista korvauksia. Pankin valvontaan tarttuvat tapaukset kertovat siitä, että järjestelmä toimii. Riski jää jonkun muun kannettavaksi. Bisnesmalli on rakennettu siten, että luottokorttiyhtiö tarjoaa suojan, jos itse huolehtii kortista ja PIN-koodista. (Kaleva 2016.)

Korttitapahtumareklamaation voi tehdä, jos

- Tiliotteella korttiostoja ja/tai automaattinostoja, joita ei ole tehnyt.
- Korttiostos on veloitettu kahteen kertaan.
- Ei ole saanut kortilla tilaamia tavaroita tai palveluita.
- Saapunut tuote on virheellinen.

- ”Kyse on sopimuksesta, joka ei kuluttajansuojalainsäädännön mukaisesti sido kuluttajaa.”
  (Nordea 2018a.)

Maksukorttien liikkeellelaskijana pankki vastaa maksupalvelulain ja korttiehtojen mukaisesti maksukortin oikeudettomasta käytöstä. Mikäli kortinhaltija on tehnyt suorituksen maksukortin credit-ominaisuudella, on pankilla lisäksi yhteisvastuu myyjän kanssa rahasuorituksen palauttamisesta kuluttajasuojalain mukaisesti. Reklamaatio tulee tehdä pankkiin, jollei asiaa saa ratkaistua myyjän kanssa. (Nordea 2018a.)

Asiaa tulisi aina ensin selvittää myyjän kanssa, jos

- ”Tapahtuma on veloitettu kahteen kertaan.”
- Tilaamia tuotteita ei ole saapunut.
- ”Tuote ei vastaa tilattua.”
- Kuluttaja on sitoutunut toistuvaan veloitukseen ja palvelu on irtisanottava.
  (Nordea 2018a.)

Kortinhaltijan on kortin katoamisen havaittuaan tehtävä katoamisilmoitus ilman perustelematonta viivytystä. Kortinhaltijan vastuu kortin käytöstä loppuu yleensä silloin, kun kuluttaja on tehnyt ilmoituksen kortin katoamisesta tai oikeudettomasta käytöstä luotonantajalle tai luotonantajan ilmoittamalle taholle. (Kilpailu- ja kuluttajavirasto 2018.)

Vastuuseen kortin katoamisesta, varkaudesta tai väärinkäytöstä voi joutua, jos

- Toimii huolimattomasti.
- ”On luovuttanut kortin ulkopuoliselle.”
- Viivyttää katoamisilmoituksen tekemistä.
  (Kilpailu- ja kuluttajavirasto 2018.)

”Huolellisesti toimiessaan kortinhaltija ei vastaa oikeudettomasta kortin väärinkäytöstä. Sen sijaan hänen lieväkin huolimattomuutensa aiheuttaa vastuun, joka rajoittuu 50 euroon. Jos hänen katsotaan toimineen tahallisesti tai törkeän huolimattomasti, hänellä on täysi vastuu.” (Kilpailu- ja kuluttajavirasto 2018.)

Maksukortin haltija voi vapautua maksuvälineen oikeudettomasta käytöstä syntyvästä vastuusta,

- ”Jos maksunsaaja ei ole asianmukaisesti varmistunut maksajan oikeudesta käyttää maksuvälinettä.”
- ”Kun palveluntarjoaja, jonka kanssa kortinhaltija on tehnyt maksuvälinettä koskevan sopimuksen, ei ole edellyttänyt maksajan vahvaa tunnistamista.”
  (Kilpailu- ja kuluttajavirasto 2018.)

”Jos maksukorttia on käytetty oikeudettomasti eikä kuluttaja ole tästä vastuussa, on pankin palautettava oikeudettoman maksutapahtuman rahamäärä hänen tililleen välittömästi ja viimeistään seuraavana työpäivänä siitä, kun se havaitsi maksutapahtuman tai sille ilmoitettiin maksutapahtumasta. Maksutiliä pitävällä pankilla on palautusvelvollisuus silloinkin, kun maksutapahtuma on käynnistetty maksutoimeksiantopalvelun tarjoajan välityksellä.” (Kilpailu- ja kuluttajavirasto 2018.)

”Jos fyysinen kortti joutuu rikollisten käsiin ja sitä käytetään oikeudettomasti, jakautuu vastuu syntyneestä vahingosta pankin ja asiakkaan välillä maksupalvelulain säännösten ja korttiehtojen mukaan. Erityisesti yrityskorteissa on erityisen tärkeätä selvittää korttiehtojen mukainen vastuunjako. Maksupalvelulain mukaan vastuu syntyneestä vahingosta on kokonaan pankilla, jos asiakkaan voidaan katsoa menetelleen huolellisesti. Jos asiakas on menetellyt kokonaisuutena arvioiden törkeän huolimattomasti tai tahallisesti, vastuu on kokonaan asiakkaalla. Mikäli asiakas ei ole ollut täysin huolellinen, muttei myöskään törkeän huolimaton, jää asiakkaan vastuulle 150 euron omavastuu ja pankin vastuulle loppuosa vahingosta.” (FINE 2018.)

Huolellisuuden arvioinnissa otetaan huomioon muun muassa seuraavia seikkoja:

- ”Miten asiakas on säilyttänyt korttiaan?”
- ”Miten kortti sekä pin-koodi ovat joutuneet rikollisen haltuun?”
- ”Kuinka pikaisesti asiakas on huomannut kortin katoamisen ja sulkenut korttinsa sulkupalvelussa?”
- ”Asiaan liittyvät muut olosuhteet.”
  (FINE 2018.)

”Ympäröivillä olosuhteilla voi olla vaikutusta siihen, miten asiakkaan tulisi huolehtia korttinsa tallella olosta ja käyttämisestä. Asiakkaan liikkuessa sellaisissa paikoissa, joissa on tungosta ja esimerkiksi muutoin korostunut taskuvarkauksien riski, tulee kortin tallella oloa seurata tavallista tarkemmin. Tällaisissa paikoissa voi myös olla perusteltua käyttää käteistä, jos esimerkiksi tunnusluvun näppäilyä on hankala suojata. Asiakas voi myös joutua kantamaan vastuun vahingoista, jotka syntyvät siitä, että asiakas on itse antautunut riskialttiiseen

tilanteeseen esimerkiksi käyttämällä pimeää taksia tai päästämällä vieraita ihmisiä kotiinsa.” (FINE 2018.)

4.4 Turvallinen maksukorttien käyttö

Maksukortin turvalliseen käyttämiseen löytyy paljon ohjeita yleisestä käytöstä verkkomaksamiseen ja aina lähimaksamiseen asti. Tiedot ovat yleensä kuitenkin useamman linkin takana. Siispä on hyödyllistä koota edellä mainittuihin osa-alueisiin liittyvät turvallisuusohjeet ja neuvot samaan paikkaan.

Ensimmäisenä on hyvä käydä läpi yleisiä maksukortteihin liittyviä turvallisuusohjeita (Nordea 2018b):

- Koskaan ei tulisi säilyttää korttia ja tunnuslukua yhdessä. Tunnusluku tulee aina opetella ulkoa. Käyttäessäsi maksukorttia esimerkiksi automaatilla, suojele tunnusluvun näppäily sivullisten katseilta. Samoin tulee toimia aina, kun näppäilet tunnusluvun.
- Älä koskaan anna kortin numeroa tai siihen liittyvää tunnuslukua puhelimitse, sähköpostitse tai muulla tavalla vaikka tiedustelija esittäytyisi pankin työntekijäksi tai poliisiviranomaiseksi.
- Maksukortille voi asettaa turvallisuutta lisäävät vuorokausikohtaiset turvarajat automaateille suoritetuille käteisnostoille ja laskujen maksuille. Rajat valitaan korttihakemuksen yhteydessä, mutta rajoja voi muuttaa esimerkiksi verkkopankissa tai asiakaspalvelussa.
- Korttia tulisi aina säilyttää yhtä huolellisesti kuin rahoja. Korttia ei saa koskaan jättää vartioimatta esimerkiksi autoon, ravintolapöytään, työ- tai hotellihuoneeseen.
- Ennen ostotositteen allekirjoitusta on hyvä tarkistaa loppusumma. Kortin käyttöä voi helposti seurata vertaamalla tositteita tiliotteeseesi tai luottokorttilaskuusi.
- On hyvä varmistaa säännöllisesti, että oma maksukortti tai -kortit ovat tallessa. (Nordea 2018b.)
- Korttiin voi asettaa maarajauksen eli käyttöeston tiettyihin maihin tai maanosiin, esimerkiksi Aasiaan. Yleensä asiakas pystyy asettamaan kortin käyttöalueen omassa verkkopankissa niissä pankeissa, joissa tämä toiminto on käytössä.
  (VertaaEnsin 2017.)
- Vanha maksukortti tai turhaksi tullut kortti tulee aina tuhota leikkaamalla se useaan osaan niin, että magneettijuova ja siru tuhoutuvat. Kortin lopettamisesta tulee aina ilmoittaa myös omaan pankkiin
  (Korttiturvallisuus 2018g).

Maksukortteja käytetään nimensä mukaisesti maksamiseen. Maksamiseen liittyy myös hyviä ja käytännöllisiä turvallisuusohjeita ja vinkkejä (Korttiturvallisuus 2018g.):

- Kortin sulkupalvelun numero on hyvä tallentaa omaan puhelimeen.
- Kuten yleisissä turvallisuusohjeissa ilmeni myös aiemmin, oston summa on tarkistettava ennen kuin sen hyväksyy tunnusluvulla tai allekirjoituksella.
- Huolehdi, että saat maksusuorituksen jälkeen oman korttisi ja kuitin itsellesi.
- Jos havaitsee tiliotteella tai laskulla veloituksia, joita ei tunnista, on oltava yhteydessä omaan pankkiin.
- Kortin takana olevaan allekirjoituspaneeliin on kirjoitettava oma nimi, sillä kaupalla on oikeus olla hyväksymättä allekirjoittamatonta korttia.
- Henkilöllisyys on todistettava korttimaksun yhteydessä niin vaadittaessa. Kyseessä on maksajan oma etu ja turvallisuus.
- Korttia ei saa koskaan luovuttaa toiselle henkilölle, ei edes oman perheenjäsenen käyttöön. Kortti ja tunnusluku ovat aina henkilökohtaisia.
- Mikäli et tarvitse jokaista korttiasi päivittäin, kannattaa pohtia kyseisen kortin jättämistä turvalliseen säilöön.
- Taskuvarkaita tulee aina varoa. Luvussa 4.2.4 on käyty läpi esimerkiksi taskuvarkaiden käyttämiä harhautus- ja varkaustapoja.
  (Korttiturvallisuus 2018g.)
- Tunnusluku tulee aina näppäillä käden tai lompakon suojassa (Korttiturvallisuus 2018e).

Kortti on turvallinen maksutapa nettimaksamisessa, kunhan maksukorttia käyttää yhtä huolellisesti kuin muussa asioinnissa. Verkkomaksamiseen löytyy niin sanottuja kultaisia sääntöjä, joilla pääsee hyvään ja turvalliseen lopputulokseen (Korttiturvallisuus 2018i):

- Älä koskaan anna maksukortin numeroa tai tunnuslukua sähköpostitse kenellekään.
- Jos ei ole tarkoituksena ostaa mitään, älä koskaan anna kortin tietoja esimerkiksi mielipidekyselyihin tai vastaaviin tiedusteluihin.
- Kortin tietoja ei saa koskaan antaa esimerkiksi sähköpostin välityksellä tuleviin ilmoituksiin, joissa kerrotaan yllättävästä arpajaisvoitosta tai palkinnosta ja pyydetään lähettämän kortin tiedot palkinnon saamiseksi.
- Jotkut Euroopan ulkopuolella toimivista verkkokaupoista saattavat pyytää kortista ja passista valokopiota esimerkiksi faksitse varmistaakseen, että tilausta tekee kortin

todellinen haltija. Korttitietoja ei saa koskaan toimittaa suojaamattomassa sähköpostissa.

- Varmista, että kortin tiedot salataan asianmukaisesti ennen tietojen lähettämistä verkossa.
  (Korttiturvallisuus 2018i.)

Itse lähimaksamisesta kerrottiin luvussa 2.3, mutta lähimaksamiseen liittyy tiettyjä turvallisuusasioita, jotka kannattaa pitää mielessä. Lähimaksukortit käyttävät NFC eli Near Field Communication -tekniikkaa, joka tarkoittaa maksukortin ja maksupäätteen välistä suojattua dataliikennettä. Ilman tunnuslukua tehtyjen lähimaksujen määrään ja kokonaisarvoihin on tehty rajoituksia. Aina välillä maksupääte vaatii myös alle 25 euron ostosten hyväksymistä tunnusluvulla. Käytännöt vaihtelevat korteittain, mutta esimerkiksi joka viides ostos tulee vahvistaa tunnusluvulla. Tarkoituksena on varmistaa, että kortti on oikean kortinhaltijan hallussa, eikä vääriin käsiin joutuneella kortilla voi tehdä useita ostoksia. Lähimaksuominaisuus lisää korttimaksamisen turvallisuutta, koska ilman tunnuslukua tehtävät maksut vähentävät mahdollisuuksia tunnusluvun urkkimiseen. Lähimaksun avulla tunnusluku ei siten joudu rikollisten käsiin. (Korttiturvallisuus 2018c.)

5 Pohdinta

Tutkimuksen tavoitteena oli vastata kysymykseen, mitkä ovat maksukorttien yleisimmät riskit. Tutkimus on suunnattu kaikille korttimaksamisesta kiinnostuneille ja erityisesti siihen liittyvien riskien hahmottamiseen. Korttimaksamisen vallatessa elintilaa käteiseltä on tärkeää tiedostaa myös siihen liittyviä harmaita puolia ja niiltä suojautumiseksi vaadittavia toimia. Alatutkimuskysymyksenä oli, miten maksukorttien riskeiltä voi suojautua. Kävimme läpi tähän liittyviä asioita itse maksukorttien turvallisuusominaisuuksien kannalta ja konkreettisten suojautumistoimenpiteiden esittelyn pohjalta.

Maksukorttien riskit pohjautuvat erilaisiin väärinkäyttökeinoihin. On tärkeää ymmärtää, mitä erilaisia mahdollisuuksia rikollisilla on korttien väärinkäyttöön, jotta voi hahmottaa maksukorttien riskejä. Olemme koonneet useita erilaisia väärinkäyttökeinoja ja niiden pohjalta analysoimme, mitä riskejä ne aiheuttavat. Riskeiltä suojautumisessa on kaksi eri puolta. Korttiyhtiöiden ja kortinmyöntäjien luomat turvallisuusominaisuudet liittyen korttimaksamiseen ja itse kortinhaltijan aktiivinen toiminta kortin turvallisen käytön edistämiseksi.

Maksukortteihin liittyviä riskejä on useita. Koemme, että seuraavat riskit pohjautuvat täysin väärinkäyttöön:

- Maksukortin tiedot kopioidaan internetin kautta jollain tavalla.
- Maksukortin tiedot kopioidaan skimmauslaitteella.
- Maksukortista valmistetaan aidonnäköinen kopio.
- Maksukortin pin-koodi urkitaan ja fyysinen kortti varastetaan.
- Maksukortilta varastetaan rahaa lähimaksupäätteellä varustetulla maksupäätteellä.
- Maksukortin tiedot saadaan kalastelulla.

Tutkimusta tehdessä havaitsimme myös muita riskejä, jotka mainitsemme tässä:

- Maksukortti ei jostain syystä toimi ja tämä aiheuttaa taloudellista tai muuta vahinkoa kortinhaltijalle.
- Maksukortti ei ole yhteensopiva, mikä pakottaa usean korttiyhtiön maksukorttiin.
- Maksukortti ei käy maksutapana, mikä pakottaa useamman maksutavan hankkimiseen ja ylläpitämiseen.

Riskeiltä suojautumiseen löytyi paljon tietoa. Korttien turvallisuusominaisuudet kehittyvät jatkuvasti ja erilaiset seurantajärjestelmät mahdollistavat riskien ehkäisemisen. Maksukortin huolellinen käyttö ja säilytys vähentää riskien toteutumista huomattavasti.

5.1 Johtopäätökset, kehitys- ja jatkotutkimusehdotukset

Mielestämme yleisimmät riskit maksukortteihin liittyen ovat maksukorttien tietojen joutuminen vääriin käsiin internetin kautta, maksukortin tietojen kopioiminen skimmauslaitteella ja maksukortin varastaminen. Nämä ovat rikollisen kaikista helpoimmat toteuttaa ja vaativat vähiten resursseja. Lisäksi nämä ovat todella yleisiä keinoja maksukortin väärinkäyttöön ja aiheuttavat vuosittain isoja taloudellisia tappioita korttiyhtiöille. Teknisenä sovelluksena maksukortti tulee aina sisältämään tietoja ja jättämään tietojälkiä, mikä mahdollistaa sen, että tietoturva-aukon syntyessä tietoja saadaan kaapattua.

Riskeiltä on kuitenkin järkevällä käytöllä mahdollista suojautua. Myös turvallisuusominaisuudet korteissa ja erilaiset valvontajärjestelmät mahdollistavat riskien minimoimisen. Jos kortinhaltija käyttää korttiaan huolellisesti, noudattaa erilaisia kehotuksia turvallisuuteen liittyen ja säilyttää korttia huolellisesti riippumatta ympäristöstä, riskeille altistumisen todennäköisyys yksittäisenä kortinhaltijana on pieni. Ja jos riskeille altistuu, vastuun vahingosta kantaa suurimmassa osassa tapauksista korttiyhtiö tai pankki.

Kehitysideoina koemme, että riskejä on yhä mahdollista pienentää ja tehdä korttimaksamisesta entistä turvallisempaa. Maksukorteissa voisi esimerkiksi olla muuttuva korttinumero tai CVC-koodi, joka mahdollistaisi sen, että tietojen joutuessa rikollisten haltuun, niillä ei välttämättä tekisi mitään. Myös erilaisten biotunnisteiden käyttö maksujen vahvistamisessa voisi lisätä turvallisuutta, esimerkiksi pin-koodin sijaan maksu vahvistettaisiin sormenjäljellä. Magneettiraidan poistaminen korteista ja siirtyminen pelkästään sirukortin käyttöön vaikeuttaisi huomattavasti korttien kopioimista. Yleinen tietoisuuden lisääminen ja tietojen koonti samaan paikkaan vähentäisi varmasti maksukorttien riskien toteutumista.

Jatkotutkimusehdotuksina koemme, että voisi tutkia, millaisia riskejä tulevaisuudessa saattaa esiintyä maksukortteihin liittyen maailman muuttuessa entistä digitaalisemmaksi ja nopeammin. Myös sitä voisi tutkia, mitkä ovat ylipäätään tulevaisuuden maksutapoja ja jäävätkö maksukortit pian vain muistoksi, kuten esimerkiksi käteinen tällä hetkellä.

5.2 Opinnäytetyöprosessin ja oman oppimisen arviointi

Opinnäytetyö oli kokonaisuudessaan pitkä projekti. Periaatteessa projekti alkoi jo syksyllä 2017, kun päätimme tehdä opinnäytetyön parityönä. Olimme jo muun muassa ryhmätöiden ansiosta tehneet paljon yhteisiä opintoihin liittyviä töitä, joten tiesimme yhteistyön onnistuvan hyvin. Jos jossain vaiheessa toisella olisi vaikeuksia saada tekstiä aikaiseksi, voisi toiselta aina pyytää apua. Myös mahdollisen motivaatiopuutteen iskiessä pystyi jo etukäteen tietämään, että pari onnistuisi antamaan tarvittavan motivaation nostatuksen.

Opinnäytetyön aihe oli lopulta yllättävän helppo valinta, kun se ensimmäisen kerran tuli mieleen. Erilaisia ideoita aiheeksi oli mietiskelty esimerkiksi lähimaksamisen turvallisuudesta tai erilaisten maksusovellusten turvallisuudesta. Kyseiset aiheet eivät kuitenkaan vaikuttaneet yhtä mielekkäiltä ja mielenkiintoisilta kuin maksukorttien riskit. Varsinkin näin finanssi- ja talousasiantuntijan koulutusohjelman opiskelijoina aihe on erittäin sopiva ja mielekäs.

Opinnäytetyöseminaarin jälkeen itse varsinainen opinnäytetyön kirjoittaminen alkoi tammikuussa 2018. Jo tuolloin ehdoton takaraja opinnäytetyön valmistumiselle oli vappu, jolloin ehtisi valmistua kesällä 2018. Tietenkin mitä aiemmin ennen vapun juhlintaa opinnäytetyön saisi valmiiksi sen parempi. Aluksi opinnäytetyötä tehtiin verkkaisella noin kerran viikossa tahdissa. Koimme, että samassa paikassa tekeminen oli tuottoisa vaihtoehto. Kuitenkin lähestyessä helmi- ja maaliskuuta pyrimme tekemään opinnäytetyötä kahdesti viikossa. Todellisen loppukirin otimme huhtikuun puolessa välissä, jolloin rutistimme huomattavan osan työstä valmiiksi. Loppurutistus ei kuitenkaan olisi ollut mahdollista ilman sitä ennen tehtyä hyvää ja kattavaa ajatustyötä. Kuuluisa sanonta ”hyvin suunniteltu on puoliksi tehty” piti hyvin paikkansa.

Miettiessä mitä tulisi tehtyä toisin, tulee ensimmäisenä mieleen, että pyrkisi heti aluksi varmistamaan haastattelun. Haastattelua pyrittiin saamaan ja se meille kerran luvattiinkin, mutta syystä tai toisesta emme koskaan saaneet vastauksia kysymyksiimme. Varsinkin luottokorttiyhtiöiltä ei saanut edes minkäänlaista vastausta lähetettyihin sähköposteihin. Toinen asia olisi aiheen muokkaaminen enemmän sellaiseksi, että aiheesta olisi saatavilla enemmän julkista tietoa. Aiheen luonteen takia on jouduttu turvautumaan suhteellisen useaan otteeseen samoihin lähteisiin.

Suurin osa riskeistä oli etukäteen tiedossa aiheen kiinnostavuuden ja koulutuksen johdosta. Skimmauksen esiintyminen vielä vuonna 2017 oli kuitenkin yllättävää. Vaikka sirukortit ovat vähentäneet skimmaukseen liittyviä riskejä Suomessa ja Euroopassa, voi pelkällä magneettijuovalla suorittaa nostoja vielä tietyissä maailmankolkissa. Puhumattakaan internetissä tapahtuvasta väärinkäytöstä esimerkiksi tietyissä verkkokaupoissa, joihon riittää pelkkä kortin numero ja turvaluku.

Lähteet

American Express 2018. Arkipäivän ostokset lähimaksulla helposti ja nopeasti. Luettavissa:
https://www.americanexpress.com/fi/fi/content/benefits/contactless.html.
Luettu 4.3.2018.

Canadacasino.net. DEBIT AND CREDIT CARD DEPOSITS. Luettavissa:
http://www.canadacasino.net/bank-cards.
Luettu: 4.3.2018.

ComputerWeekly.com 2008. How banks are detecting credit fraud? Luettavissa:
http://www.computerweekly.com/feature/How-banks-are-detecting-credit-fraud.
Luettu: 8.3.2018.

FA 2017. Finanssiala. Säästäminen, luotonkäyttö ja maksutavat. Tekstiraportti 2017. Finanssiala. Luettavissa:
http://www.finanssiala.fi/materiaalit/SLM_2017_Tutkimusraportti.pdf#search=maksutapa.
Luettu: 5.2.2018.

Finanssivalvonta 2016. Maksukortin käyttö edellyttää huolellisuutta. Luettavissa:
http://www.finanssivalvonta.fi/fi/Finanssiasiakas/Finanssialan_palveluita/Maksupalvelut/Maksuvalineet/Maksukortit/Pages/Default.aspx.
Luettu: 23.1.2018.

FINE 2017. Vastuu maksukortin oikeudettomasta käytöstä – Ratkaisukäytäntöä pankin ja asiakkaan välisestä vastuunjaosta. Vakuutus- ja rahoitusneuvonta. Luettavissa:
https://www.fine.fi/media/julkaisut-2017/vastuu-maksukortin-oikeudettomasta-kaytosta-2017.pdf.
Luettu: 23.2.2018.

FINE 2018. Tilinkäyttö ja maksaminen. Luettavissa:
https://www.fine.fi/finanssitietoa/pankkiasiat/tilinkaytto-ja-maksaminen.html.
Luettu: 13.4.2018.

Helsingin Uutiset 2016. Katuhuijarien 10 yleisintä konstia – älä lankea näihin. Luettavissa:
https://www.helsinginuutiset.fi/artikkeli/390857-katuhuijarien-10-yleisinta-konstia-ala-lankea-naihin.

Luettu 13.4.2018.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 1997. Tutki ja kirjoita. Tammi. Helsinki.

IL 2017. Satojentuhansien pankkikorttien tiedot vaarassa lähimaksujen takia - katso videolta, miten. Luettavissa:
http://www.iltalehti.fi/uutiset/201702062200064688_uu.shtml.
Luettu 23.2.2018.

Investopedia 2018. Data Breach. Luettavissa:
https://www.investopedia.com/terms/d/data-breach.asp.
Luettu: 27.2.2018.

IS 2017. Rikolliset kehittivät pirullisen tavan viedä maksukortin tiedot kylmäasemalla – näin tunnistat skimmauslaitteen. Luettavissa:
https://www.is.fi/kotimaa/art-2000005328494.html.
Luettu: 13.4.2018.

IS 2018. Poliisi tutkii laajaa skimmaussarjaa – suomalaisten pankkikortteja käytetty Indonesiassa: ”Hyvin hankala puuttua”. Luettavissa:
https://www.is.fi/kotimaa/art-2000005619486.html.
Luettu: 13.4.2018.

Kaleva 2016. Tililtä katosi hetkessä 2 972 euroa – ti-li-ta-pah-tu-mis-ta paljastui karu totuus. Luettavissa:
http://www.kaleva.fi/uutiset/kotimaa/tililta-katosi-hetkessa-2-972-euroa-tilitapahtumista-paljastui-karu-totuus/730897/.
Luettu: 13.4.2018.

Karjalainen 2015. Kuka maksaa viulut, jos luottokortin tiedot kaapataan? - kuluttajalle hyviä uutisia. Luettavissa:
https://www.karjalainen.fi/uutiset/uutis-alueet/kotimaa/item/86614-kuka-maksaa-viulut-jos-luottokortin-tiedot-kaapataan-kuluttajalle-hyvia-uutisia.
Luettu: 13.4.2018.

Kauppalehti 2016. Näin maksaminen muuttuu - maksukortti katoaa, käteinen jää historiaan. Luettavissa:

https://www.kauppalehti.fi/uutiset/nain-maksaminen-muuttuu---maksukortti-katoaa--kateinen-jaa-historiaan/xGRmPdts.
Luettu: 23.1.2018.

Kilpailu- ja kuluttajavirasto 2018. Maksukortin katoaminen.
Luettavissa:
https://www.kkv.fi/Tietoa-ja-ohjeita/Maksut-laskut-perinta/maksukortin-katoaminen/.
Luettu: 13.4.2018.

Korttiturvallisuus 2018a. Haittaohjelmat. Luettavissa:
https://www.korttiturvallisuus.fi/Verkossa/Haittaohjelmat/.
Luettu 21.2.2018.

Korttiturvallisuus 2018b. Kalastelu ja huijaukset. Luettavissa:
https://www.korttiturvallisuus.fi/Verkossa/Huijausviestit/.
Luettu: 16.2.2018.

Korttiturvallisuus 2018c. Lähimaksaminen. Luettavissa:
https://www.korttiturvallisuus.fi/Lahimaksaminen/.
Luettu 13.4.2018.

Korttiturvallisuus 2018d. Maantieteellinen aluerajaus. Luettavissa:
https://www.korttiturvallisuus.fi/Matkoilla/Geoblocking/.
Luettu: 23.2.2018.

Korttiturvallisuus 2018e. Maksaminen. Luettavissa:
https://www.korttiturvallisuus.fi/Kaupassa/Maksaminen/.
Luettu: 13.4.2018.

Korttiturvallisuus 2018f. Mobiilimaksaminen. Luettavissa:
https://www.korttiturvallisuus.fi/Ajankohtaista/Mobiilimaksaminen/.
Luettu: 16.2.2018.

Korttiturvallisuus 2018g. Turvallisuusohjeita. Luettavissa:
https://www.korttiturvallisuus.fi/Kaupassa/Turvallisuusohjeita/.
Luettu 13.4.2018.

Korttiturvallisuus 2018h. Verified by Visa ja MasterCard SecureCode. Luettavissa:

https://www.korttiturvallisuus.fi/Verkossa/Todentamispalvelut/.
Luettu: 23.2.2018.

Korttiturvallisuus 2018i. Verkossa. Luettavissa:
https://www.korttiturvallisuus.fi/Verkossa/.
Luettu: 13.4.2018.

Korttiturvallisuus 2018j. Väärinkäytöstä ilmoittaminen. Luettavissa:
https://www.korttiturvallisuus.fi/Apua/Vaarinkaytosta-ilmoittaminen/.
Luettu: 21.2.2018.

Kuluttajaliitto 2018. Maksukortit. Luettavissa:
http://www.kuluttajaliitto.fi/tietopankki/oman-talouden-hallinta/maksaminen-ja-kuitit/maksu-kortit/.
Luettu: 23.1.2018.

Laki24.fi 2018a. Lievä maksuvälinepetos. Luettavissa:
https://www.laki24.fi/riri-rikokset-maksuvalinerikokset-lieva_maksuvalinepetos/.
Luettu 27.2.2018.

Laki24.fi 2018b. Maksuvälinepetos. Luettavissa:
https://www.laki24.fi/riri-rikokset-maksuvalinerikokset-maksuvalinepetos/.
Luettu 27.2.2018.

Laki24.fi 2018c. Törkeä maksuvälinepetos. Luettavissa:
https://www.laki24.fi/riri-rikokset-maksuvalinerikokset-torkea_maksuvalinepetos/.
Luettu 27.2.2018.

MasterCard Card Security Features 2015. Luettavissa:
https://www.nets.eu/globalassets/documents/cross-border-and-other-english-doc/fraud-secure-payments/mastercard-card-security-fact-sheet-070915.pdf.
Luettu: 27.2.2018.

MobilePay 2018. FAQ. Luettavissa:
https://www.mobilepay.fi/fi-fi/Pages/faq.aspx.
Luettu: 16.2.2018.

MTV 2012. Suomalaisten korttitietoja käytettiin Chicagossa – Vahingot kymmeniä tuhansia. Luettavissa:
https://www.mtv.fi/uutiset/rikos/artikkeli/suomalaisten-korttitietoja-kaytettiin-chicagossa-vahingot-kymmenia-tuhansia/2046310#gs.mcTc5=k.
Luettu: 13.4.2018.

MTV 2013. Tältä näyttää pankkikortin kopioiva skimmauslaite. Luettavissa:
https://www.mtv.fi/uutiset/rikos/artikkeli/talta-nayttaa-pankkikortin-kopioiva-skimmauslaite/2053210#gs.87xuxgA.
Luettu: 4.3.2018.

MTV 2016. Maksuvälinepetosten määrä räjähti – 175 prosenttia enemmän kuin viime vuonna. Luettavissa:
https://www.mtv.fi/uutiset/rikos/artikkeli/maksuvalinepetosten-maara-kasvaa-175-prosenttia-enemman-kuin-viime-vuonna/5851616#gs.Muzlcjo.
Luettu: 4.3.2018.

MyNewsDesk 2017. Mobiilimaksamisen suosio kasvaa – suomalaiset kokevat sen turvalliseksi ja 74 % on käyttänyt mobiililaitettaan maksamiseen. Luettavissa:
http://www.mynewsdesk.com/fi/visa-europe-suomi/pressreleases/mobiilimaksamisen-suosio-kasvaa-suomalaiset-kokevat-sen-turvalliseksi-ja-74-percent-on-kaeyttaenyt-mobiililaitettaan-maksamiseen-2182956.
Luettu: 4.3.2018.

Nets 2016. Kortti mieluisin maksutapa. Luettavissa:
https://www.nets.eu/fi-fi/uutiset-ja-tiedotteet/Pages/Suomalaiset-Pohjolan-k%C3%A4teiskansaa,-kortti-silti-mieluisin-maksutapa.aspx?utm_campaign=unspecified&utm_content=unspecified&utm_medium=email&utm_source=apsis-anp-3.
Luettu: 5.2.2018.

Nets 2018. Korttiturvallisuuspalvelu. Luettavissa:
https://www.nets.eu/fi-fi/palvelut/kortit/ohjeita/Pages/Turvallisuus.aspx.
Luettu: 8.3.2018.

Nordea 2017. Varo tietojenkalastelua. Luettavissa:
https://www.nordea.com/fi/media/uutiset-ja-lehdistotiedotteet/News-fi/2017/2017-11-30-varo-tietojenkalastelua.html.

Luettu: 21.2.2018.

Nordea 2018a. Korttireklamaatio. Luettavissa:
https://www.nordea.fi/henkiloasiakkaat/palvelumme/maksu-luottokortit/korttireklamaatio.html.
Luettu: 13.4.2018.

Nordea 2018b. Ohjeita kortin turvalliseen käyttöön. Luettavissa:
https://www.nordea.fi/henkiloasiakkaat/palvelumme/maksu-luottokortit/kortin-turvallinen-kaytto.html.
Luettu 13.4.2018.

Oxen Technology 2016. Spear Phishing: A New Twist on An Old Scam. Luettavissa:
https://oxen.tech/blog/spear-phishing-new-twist-old-scam/.
Luettu: 4.3.2018

PCI Security 2018. Luettavissa:
https://www.pcisecuritystandards.org/pci_security/.
Luettu: 27.2.2018.

Poliisi 2018. Maksukorttirikollisuus on kasvava rikosilmiö. Luettavissa:
https://www.poliisi.fi/rikokset/rikosilmioita/maksukorttirikollisuus
Luettu 16.2.2018.

Profit 2015. Katoaako käteinen? Luettavissa:
https://profit.lindorff.fi/katoaako-kateinen/.
Luettu: 23.1.2018.

SP 2017. Suomen Pankki. Käteisen käyttö ja saatavuus. Maksuneuvoston kokous. Suomen Pankki. Luettavissa:
https://www.suomenpankki.fi/globalassets/4_takala_kari_kateisen-kaytto-ja-saatavuus.pdf.
Luettu 23.1.2018.

SP 2018. Suomen Pankki. Taulukot. Luettavissa:
https://www.suomenpankki.fi/fi/Tilastot/maksuliiketilastot/taulukot/.
Luettu 22.3.2018.

Taloustaito 2017. Maksukortti matkalla – maksa kortilla turvallisesti. Luettavissa: https://www.taloustaito.fi/vapaalla/maksukortti-matkalla--maksa-kortilla-turvallisesti/. Luettu: 30.3.2018

Tilastokeskus 2017a. Tietoon tulleiden seksuaalisten ahdistelujen määrä väheni 22,6 prosenttia, raiskauksien määrä kasvoi 6 prosenttia. Luettavissa: http://tilastokeskus.fi/til/rpk/2017/04/rpk_2017_04_2018-03-16_tie_001_fi.html. Luettu 6.4.2018.

Tilastokeskus 2017b. Tietoon tulleiden seksuaalirikoksien määrä kasvussa: Luettavissa: http://tilastokeskus.fi/til/rpk/2016/04/rpk_2016_04_2017-01-19_tie_001_fi.html. Luettu 6.4.2018.

TM 2017. TM testasi: Pankkikortilla tapahtuvasta lähimaksusta löytyi tietoturvauhka – näin voro voi käyttää sitä hyväksi. Luettavissa: https://tekniikanmaailma.fi/tm-testasi-pankkikortilla-tapahtuvasta-lahimaksusta-loytyi-tietoturvauhka-nain-voro-voi-kayttaa-sita-hyvaksi/. Luettu: 23.2.2018.

VertaaEnsin 2016. Suomessa suuri maksuvälinepetosvyyhti. Luettavissa: https://www.vertaaensin.fi/blog/maksuvalinepetos. Luettu: 13.4.2018

VertaaEnsin 2017. Maksukortin suojaus. Luettavissa: https://www.vertaaensin.fi/luottokortti/opas/maksukortin-suojaus. Luettu: 13.4.2018.

Yle 2014a. Hakkerit vievät jättimäisiä määriä luottokorttitietoja. Luettavissa: https://yle.fi/aihe/artikkeli/2014/09/25/hakkerit-vievat-jattimaisia-maaria-luottokorttitietoja. Luettu: 13.4.2018.

Yle 2014b. Rahan historiaa. Luettavissa: https://yle.fi/aihe/artikkeli/2012/10/25/rahan-historiaa. Luettu: 23.1.2018.

Yle 2017a. Pankkikorttitietoja päätynyt huijareille: "Huomasin eilen, että tililtäni oli nostettu yli 80 euroa Kiinassa". Luettavissa: https://yle.fi/uutiset/3-9939151.

Luettu: 13.4.2018.

Yle 2017b. Poliisi tutkii maksuvälinepetosta Salossa – huoltoasemalta löytyi skimmauslaite. Luettavissa:
https://yle.fi/uutiset/3-9481390.
Luettu: 13.4.2018.